吞吐量(Throughput):路由器每秒能处理的数据包个数,通常以PPS(Packet Per Second)为单位,用于描述路由器处理和转发数据包的能力,是路由器性能描述的重要指标。

路由表容量:路由器依赖于路由表确定包转发路径,路由表容量则是指路由表可容纳的记录数量,该指标也是路由器性能的重要指标。

可靠性:用于描述设备保持稳定运行的能力,路由器设备为 24 小时运行设备,对设备可靠性要求极高。路由器通常包含冗余的配置,如接口冗余、电源冗余、系统板冗余等,用于增强设备的稳定性和可靠性。

丢包率:该指标是由于路由器的超负荷运行而导致无法转发的数据包所占所有数据包的百分比,用于描述路由器在超负荷运行状态下的性能。

2.3.5 路由器的接口介绍

通常,对于非模块化设计的路由器,其结构为固定编号,可由接口类型后加接口编号进行表示,例如 Ethernet 0、FastEthernet 1、Serial 0 等,或简单描述为 e0、f1、s0 等。

而模块化的设备,其接口则由接口类型 插槽号/接口号进行表示,例如 Ethernet 0/0 FastEthernet 0/1 Serial 1/1 等,或简单描述为 e0/0 f0/1 s1/1 等。

路由器常见接口描述如下。

1. RJ-45 接口

RJ-45 接口为最常见的以太网接口,使用双绞线进行连接。由于路由器主要用于网络互联、数据处理和网络管理,而不是用于终端接入,所以提供的 RJ-45 接口数量很少。通常,不同级别的路由器提供的 RJ-45 接口速率也不同。按照速率的不同,通常可分为如下 5 类 RJ-45 接口。

- 10Base-T:10M 传输速率的 RJ-45 接口,通常简写为 ETH 接口。
- 10/100 Base-TX:10/100M 自适应百兆以太网接口(FastEthernet),可简写为 FE 接口。
- 10/100/1000 Base-T:10/100/1000 兆自适应以太网端口。
- 1000 Base-T:千兆以太网接口(GigaBitEthernet),通常简写为 GE 接口。
- 10GE:万兆以太网接口。

其中,较为常见的是 FE 接口、10/100/1000M 自适应接口和 GE 接口,分别如图 2-50 所示。

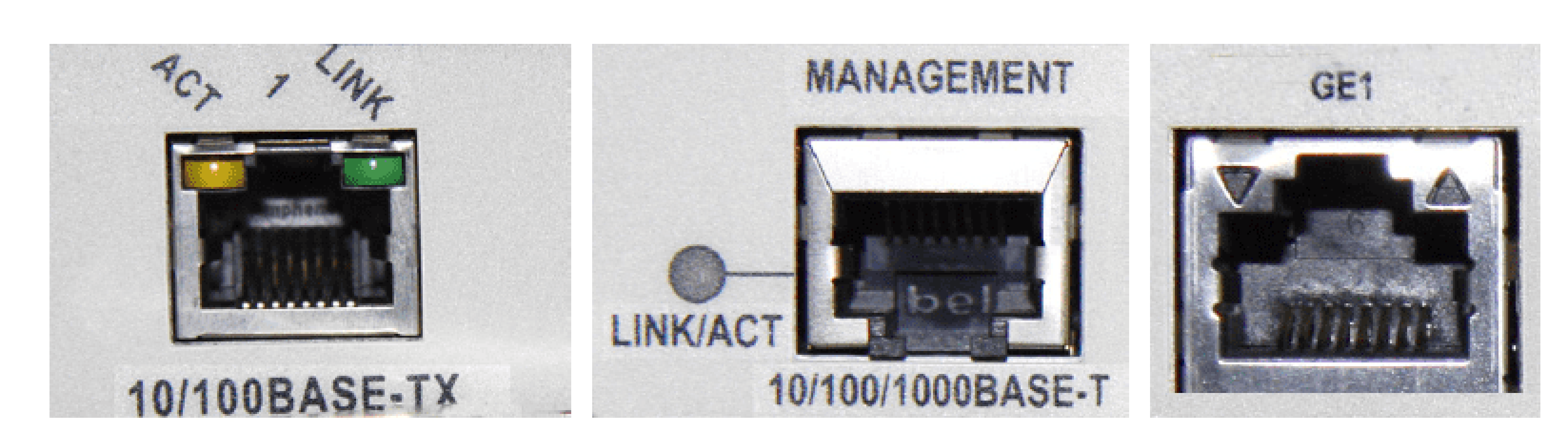


图 2-50 各种速率的路由器接口

RJ-45 接口的运行状态通常由 1 个或 2 个状态灯进行显示。

1 个状态灯:状态灯闪烁,则表示该接口状态为激活状态。如果显示为橘黄色灯闪烁,

则表示其接口当前传输速率为 10Gbps～100Gbps，而显示绿色灯闪烁，则表示当前传输速率为 1000Gbps。

2 个状态灯：绿色状态灯常亮，则表示连接为激活状态，而黄色闪烁，则表示有数据交互。

2. AUI 接口

AUI（Attachment Unit Interface，连接单元接口）是一个 D 行 15 针接口，路由器通过该接口连接粗同轴电缆。目前这种接口在局域网中并不多见，但在一些大型企业网络中仍有一些连接粗同轴电缆的应用。提供 AUI 接口的路由器板卡如图 2-51 所示。

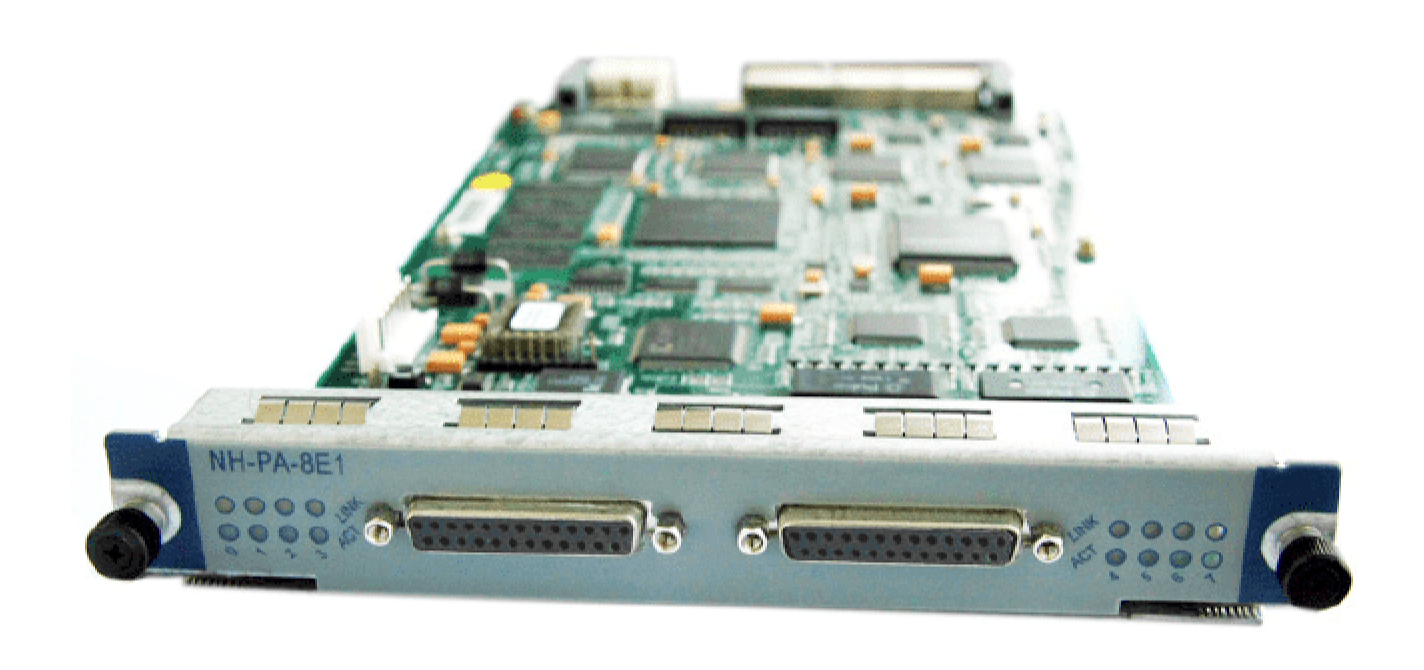


图 2-51　提供 AUI 接口的路由器板卡

3. AUX 和 Console 接口

AUX 和 Console 接口的功能相同，都是用于对路由器进行配置。AUX 接口主要用于远程配置，计算机通过 Modem 拨号连接路由器进行登录配置。而 Console 接口用于本地直接将计算机连接路由器进行配置。该两个接口通常同时出现在路由器中，如图 2-52 所示。

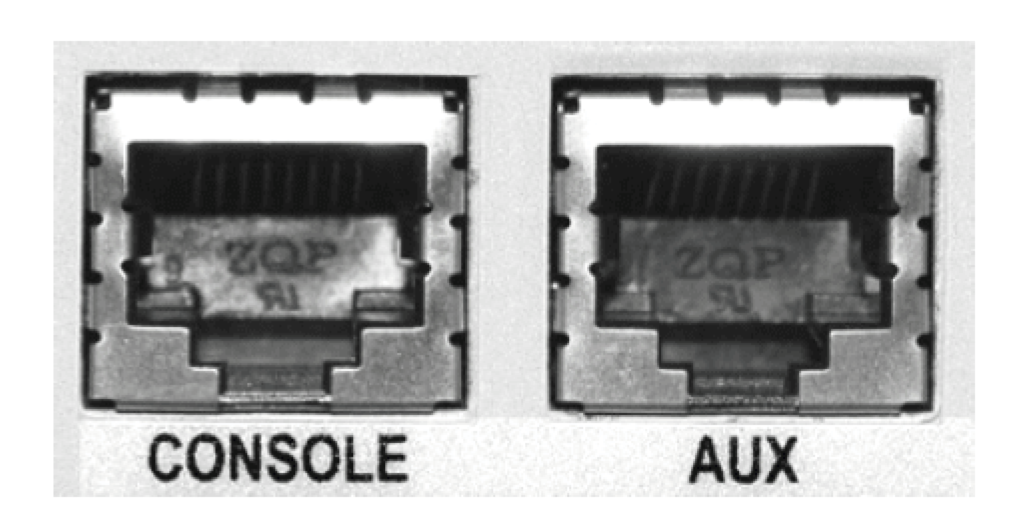


图 2-52　路由器中的 Console 和 AUX 接口

4. Serial 高速同步串口

Serial 接口属于广域网接口，在局域网中很少出现该接口。通常用于路由器连接路由器，实现广域网之间的互联。该接口所提供的数据传输速率非常高，用于实现该端口两侧所连接网络的高速同步，该接口如图 2-53 所示。

图 2-53　Serial 高速同步串口

5. ASYNC 异步串口

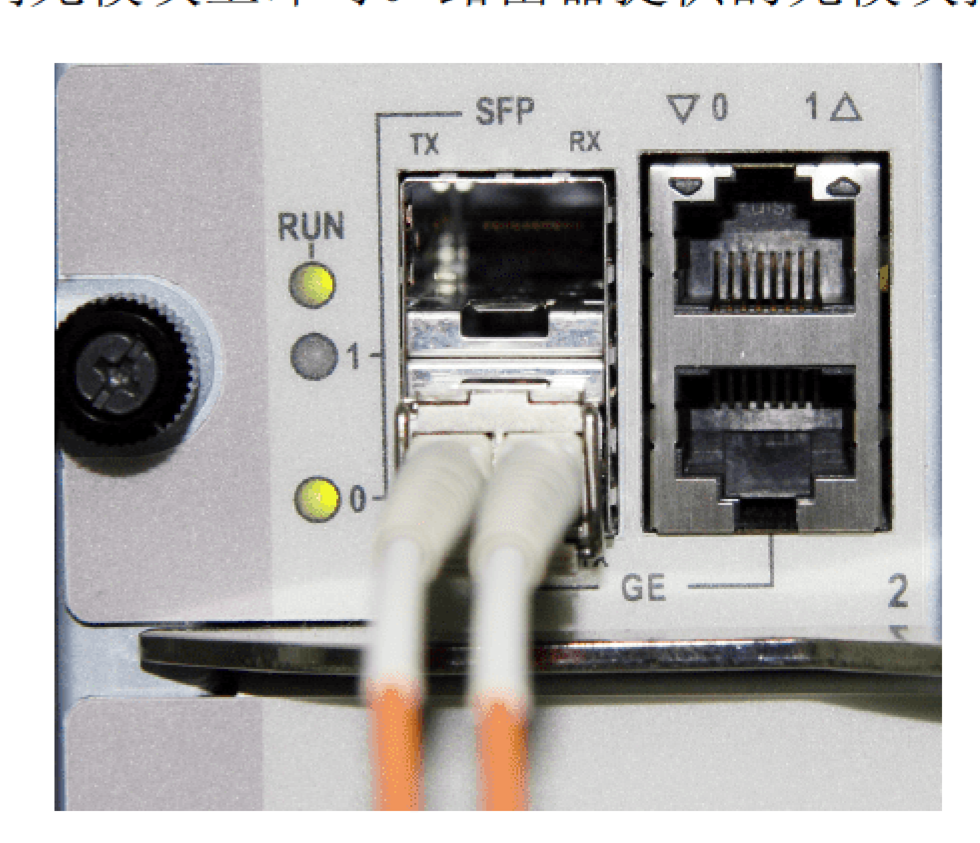
ASYNC 异步串口同样属于广域网接口，主要是用于接入 Modem 或 Modem 池，用于实现远程计算机终端通过公用电话网拨入互联网，该接口如图 2-54 所示。



图 2-54　ASYNC 异步串口板卡

6. 光模块接口

路由器中的光纤接口，可连接 SC 类型或 LC 类型的光纤。其中，SC 类型的板卡由于占空间较大，已极少使用。而 LC 类型的接口，只需要插入小巧的光模块，再将 LC 光纤连接到光模块上即可。路由器提供的光模块插口和光模块连接方式分别如 2-55 所示。



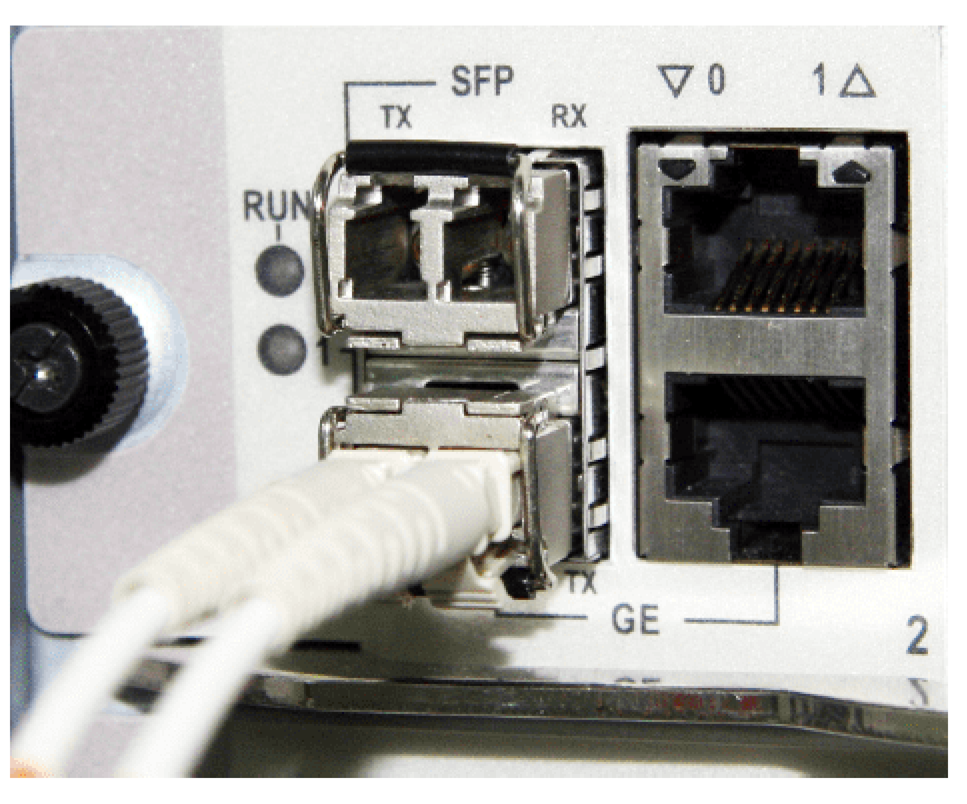


图 2-55　路由器提供的光模块插口和光模块连接方式

2.3.6　路由器的访问和配置

与交换机的访问和配置方式相同，同样可采用本地或远程的方式登录路由器设备进行

配置。在介绍交换机的小节已经详细描述，此处简单回顾。

本地访问：通过计算机的 COM 口连接路由器设备的 Console 配置口，使用超级终端或 SecureCRT 等其他客户端程序，登录路由器进行配置。

Telnet 或 SSH 访问：如果需要远程访问路由器设备，可在命令提示符中使用 Telnet 命令访问，或在 SecureCRT 等客户端程序中使用 SSH 数据加密传输模式进行访问。

FTP 方式：通过命令提示符中使用 FTP 命令或使用 FTP 客户端程序登录路由器，并上传配置文件以实现对路由器的配置、升级或文件备份。

Web 页面和网管程序配置：可通过 Web 登录并配置路由器，或通过客户端网管程序监测路由器运行状态。

2.3.7 家用型路由器

家用型路由器包括普通路由器和无线路由器。普通路由器主要提供两个功能：扩展多用户接入互联网和代理自动拨号业务。而无线路由器除该两个基础功能外，还提供无线接入互联网功能，但需要配置路由器开启无线接入功能。家用型的无线路由器相比普通路由器多了用于接收信号的天线，如图 2-56 所示。

图 2-56 家用型无线路由器

普通的家用 ADSL 宽带业务只提供了单个用户接入功能。如需要扩展用户，使得多台计算机共享一根 ADSL 线路上网，那么就需要使用路由器的路由功能。同时，在 ADSL 用户连接互联网时，每次都需要通过“宽带连接”进行拨号操作，才能接入互联网，而增加了路由器设备后，可将账号和口令配置到路由器设备中，只需开启路由器，即可自动拨号。

2.4 防火墙介绍

2.4.1 防火墙的概念介绍

防火墙（Firewall），就是用于将公众互联网与内网实现安全隔离的技术。防火墙对流经网络的数据进行扫描，允许正常合法的访问，过滤攻击和非法的数据。其最主要的目的和功能，就是在网络边界建立一个安全控制点，通过配置安全策略允许、拒绝或重定向数据流，实现对内网用户的保护。

防火墙可按照协议、服务或端口来设置安全防护策略，实现访问控制。同时，防火墙还能对网络的访问进行监控和审计，生成日志信息和统计信息，以及在遭到非法攻击时，进行报警通知。除此之外，防火墙还包括其他一些扩展功能，例如 NAT 转换技术、VPN 加密通道技术、数字证书及身份验证等。防火墙设备如图 2-57 所示。



图 2-57　Cisco 品牌的防火墙设备展示

防火墙设备仍是目前最主要的安全防护设备，除此之外，还有一些入侵主动检测设备、VPN 设备、安全网关、Web 防篡改设备、垃圾邮件防护设备、杀毒服务器等，这些同样为安全类设备，用于辅助防火墙构建更为完整的防护结构。

注意：防火墙两端所连接的网络之间所有数据流都必须流经防火墙，且只有符合安全防护策略的数据流才能够通过。

2.4.2　防火墙的分类

防火墙从其形态进行分类，大致可分为如下两大类：

- 硬件防火墙；
- 软件防火墙。

硬件防火墙是将防护程序写入到硬件芯片中，再加上操作系统、CPU、接口和存储部件就组成了硬件防火墙。硬件防火墙设备针对型强，处理数据效率高，通常部署在外部网络和内部网络之间，用于实现整体内部网络的防护。常见的硬件防火墙产品包括 Cisco、NetScreen、CheckPoint 等品牌，以及国内的东软、H3C、天融信等。

软件防火墙则是通过软件的方式实现安全防护的功能。软件类防火墙又可分为企业级防火墙和个人计算机防火墙。企业级防火墙（例如微软 ISA 防火墙）安装在服务器中，提供了友好的配置界面。该服务器便成为了软件与硬件相结合的防火墙。同样所有内外网交互的进出数据都需要流经该软件防火墙。但该类软件防火墙在网络负载较重容易成为网络瓶颈，且受到操作系统的制约，故障率也较高。而个人计算机防火墙则安装在计算机终端，仅实现对本机的防护，它将占用计算机的资源。较为成功的软件防火墙有卡巴斯基和 ZoneAlarm，以及国内的天网和瑞星个人防火墙等。

防火墙按照其技术方式则大致可分为 4 类。

- 分组过滤型（Packet filtering）；
- 应用级网关（Application Level Gateways）；
- 应用程序代理型（Application Proxy）；
- 自适应代理技术（Adaptive Proxy）。

分组过滤型即包过滤方式防火墙，该技术是第一代防火墙所采用的技术。防护策略根据数据包的源\目的 IP 地址、端口、协议等，判断对数据包进行丢弃或允许通行。

应用级网关型防火墙根据网络服务的协议判断使用数据包过滤策略，并对数据包进行

分析、统计等手段。该类防火墙与包过滤类型防火墙有一个共同点，都是依靠特定的逻辑判断是否丢弃或允许数据包通行。

应用程序代理型防火墙不允许内网用户与外网之间建立通信，而是针对内网所需服务建立对应的代理程序。所有连接的建立和数据的交互都通过代理程序进行处理。这些被代理的程序或服务包括 HTTP、SMTP、POP3、TELNET 和 FTP 等。

自适应代理技术防火墙，也就是复合型的防火墙。结合了代理技术的安全性和包过滤技术的高速率特性，是一种智能型的防火墙，可根据配置情况自行判断和决定使用代理完成服务请求还是通过网络层转发数据包。该类型防火墙在处理速度和安全性方面都有较大的提高。

注意：目前的硬件防火墙都朝着一体化安全网关（Unified Threat Management ，UTM）的方向发展。UTM 除了防火墙的控制功能外，还集成了扩展功能，例如垃圾邮件拦截、入侵检测、用户认证、双机热备等。

2.4.3 防火墙重要指标参数

吞吐量：该指标是衡量防火墙处理数据包能力的一项重要指标。具体指记录单位时间内通过防火墙设备的数据包数量。中小型的企业通常选择吞吐量为百兆级别的防火墙，便能够满足需要。

最大连接建立速率：指单位时间内防火墙与主机设备能够同时建立的最大连接数。该指标用于描述防火墙更新状态表的速率，反映了设备的实时响应能力。

并发连接数：指防火墙设备能够同时处理的最大连接数量。用于描述防火墙对多个连接的控制能力，直接影响着防火墙能够支持的最大终端数量。通常，中低端的防火墙能够支持 500～1000 连接数，而高级别的能够支持多达上万、数十万的连接数。

2.4.4 防火墙的接口

硬件的防火墙设备通常包含 3 种接口，分别是 WAN、LAN 和 DMZ 接口。

- WAN 接口：用于连接外部网络的接口，通常就是指互联网。
- LAN 接口：用于连接内部网络的接口，用于保护内部网络，如以太网、快速以太网、千兆以太网等。
- DMZ 接口：DMZ 即隔离区（Demilitarized Zone），该接口用于建立一个可信任的中间区域，既不属于外部网络也不属于内部网络。它用于放置需要开放外部访问的服务器，该区域受到防火墙的保护，同时又与内网隔离。

2.4.5 防火墙工作模式

防火墙可工作在 3 种模式下，如下：

- 路由模式；
- 透明模式；
- 混合模式。

路由模式：即防火墙内外端口所连接的两个网络必须位于不同的网段中，两个网络通过路由转发的方式实现通信。如果防火墙还带有 DMZ 接口，那么外网、内网、DMZ 区 3 个网络都必须设置不同网段的 IP 地址，否则相互之间将无法通信。

透明模式：防火墙设备对于外网、内网或路由器而言是完全透明的，使用该模式就避免了重新配置不同的网络结构，即可实现不同子网间的通信，但同时也要求内网和外网是处于同一网段之内。需要注意的是，透明模式下，防火墙的包检测、过滤机制同样发挥着作用。

混合模式：在路由模式下，需对 3 种接口及其所连接子网设置 IP 地址，而透明模式不需要对接口设置 IP 地址。如果防火墙能够同时工作在该两种模式下，那么就属于混合模式。例如，局域网中启动了 VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议），即存在主备两台防火墙作为网关，当主设备发生故障时，由另一台备设备立即接替主设备工作，以实现冗余的目的。那么启动 VRRP 协议的防火墙需要设置 IP 地址，则工作于路由模式；同时，两台防火墙之间还需互联，互联接口可通过 Hub 或交换机进行连接，并不需要设置 IP 地址，于是互联接口又工作于透明模式，这两种模式的公用，即混合模式。

2.4.6 硬件防火墙安全防护模式

在介绍防火墙设备防护结构之前，首先介绍一个重要的概念——DMZ，通常也称为“非军事化区域”。

DMZ 概念经常与防火墙同时出现。建立 DMZ 区域的目的是为解决安装防火墙设备后，外部网络无法访问内部网络中的服务器问题。内网中的一些服务器，如 Web 服务器、FTP 服务器、邮箱服务器等，这些服务器需要位于防火墙的防护之下，但同时又要满足外部网络的访问。非军事化区域，则提供了这样一个位于外部网络和内部网络之间的可访问安全区域。

内部网络同样处于防火墙的保护之下，但却与外部网络完全隔离。该区域类似于军事化管理的区域，外部网络不能直接访问该区域。一个 DMZ 结构的网络可分为 3 个区域：外部网络、DMZ 中间区域和内部网络。

以下内容，分别介绍防火墙在网络中的布放位置和防火墙设备的安全防护结构。

1. 防火墙保护内部网络

该结构下，将防火墙至于内部网络前方，仅保护内部网络，而公共服务器则不在防火墙设备的保护范围内，所以服务器将非常容易受到网络攻击和入侵。该结构仅适合于没有公共服务器的小型网络，其结构如图 2-58 所示。

2. 防火墙保护服务器和内网

该结构下，将防火墙至于服务器和内网计算机之前，服务器则作为内网计算机的一部分，防火墙同时保护了服务器和内网计算机。此时，在防火墙上需要开放一些用于访问服

务器的端口和协议，这些端口及协议的开放，极大地降低了内网的安全性，来自外部网络的攻击将有可能直接入侵服务器和计算机终端。该结构同样适用于不提供公共服务的小型网络，其结构如图 2-59 所示。

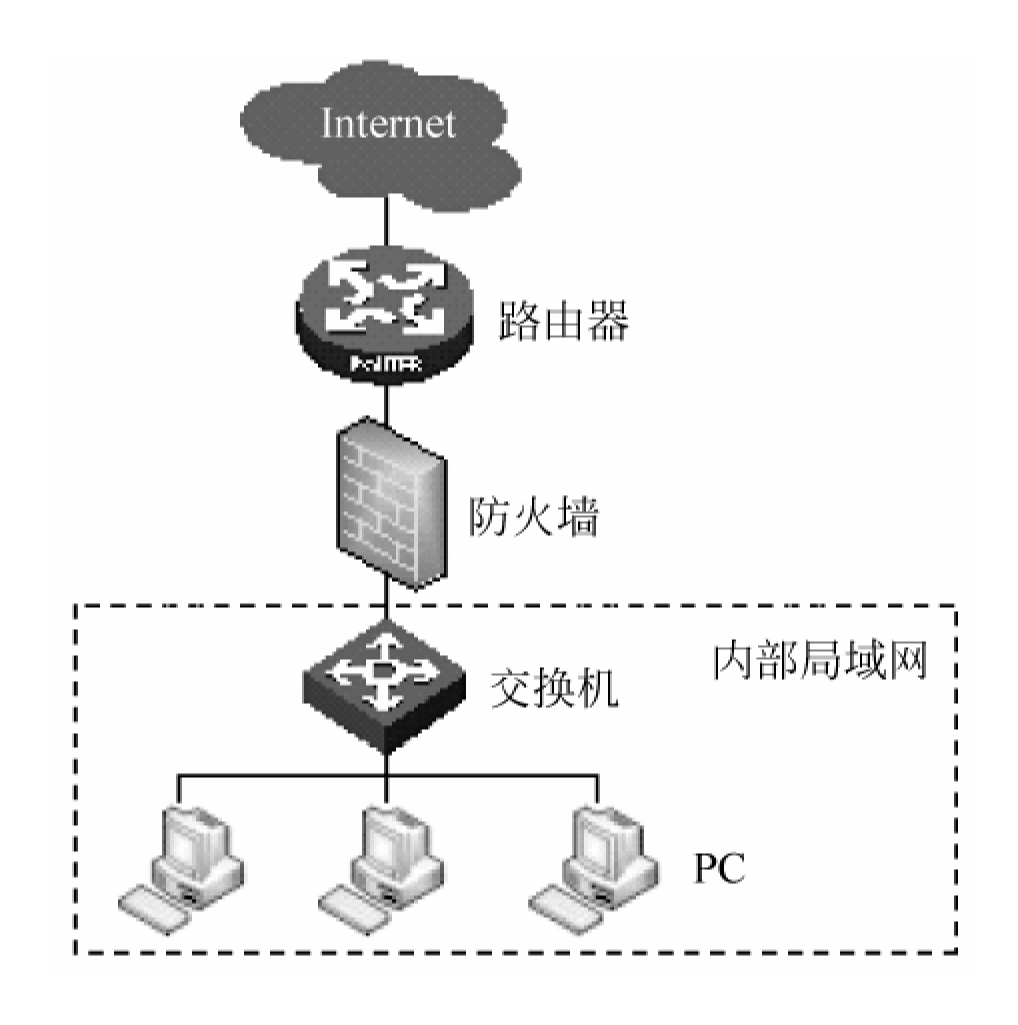


图 2-58　防火墙保护内部局域网

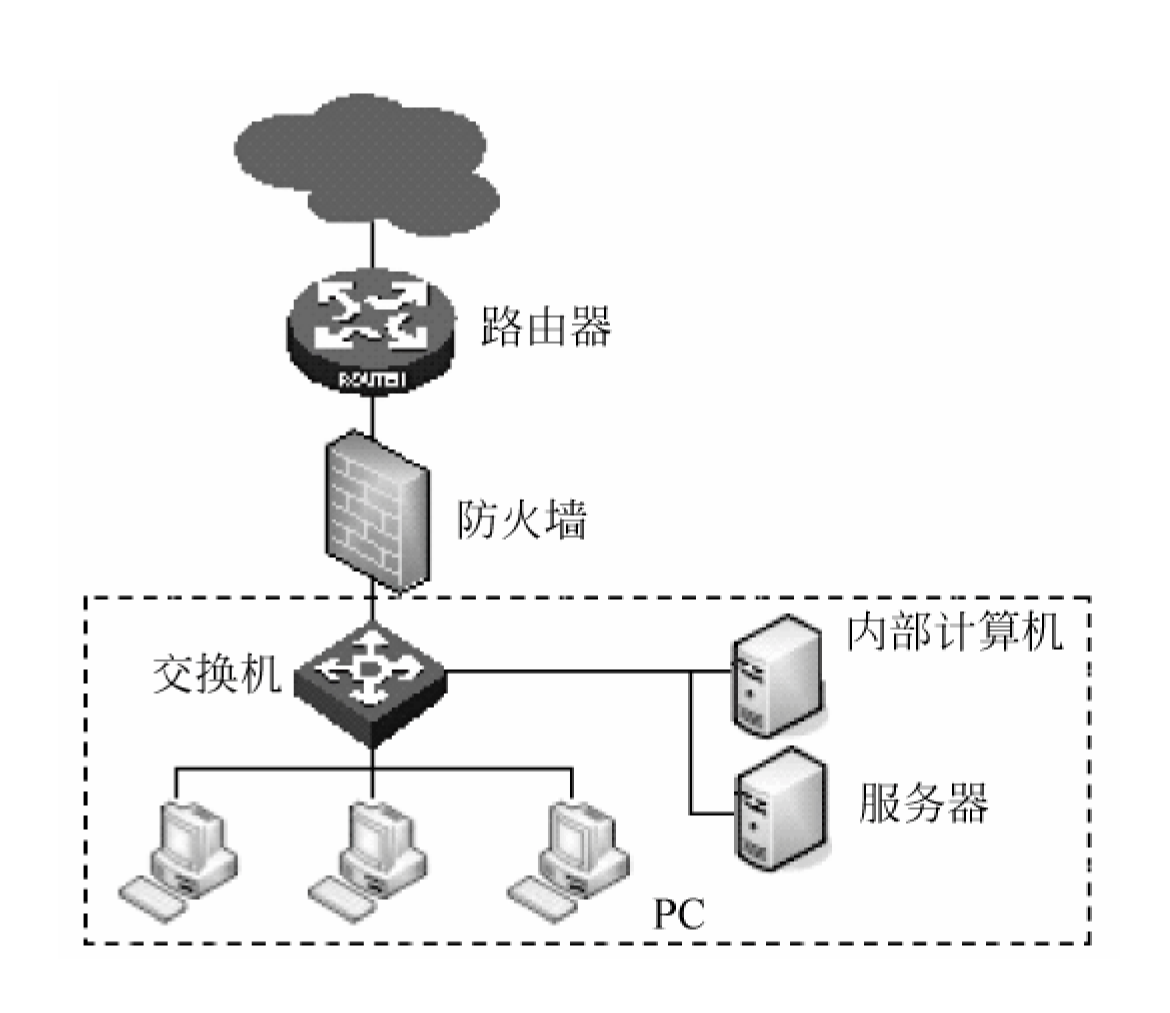


图 2-59　防火墙保护内部局域网计算机和服务器

3．火墙构建 DMZ 保护模式

该结构下，防火墙同样位于服务器和内网计算机之前，同时保护服务器和内网计算机。但不同的是，防火墙通过不同端口或特殊功能，为服务器单独构建了一个 DMZ 区域，即可供外部访问，又与内部网络计算机相互隔离，也就是形成了一个缓冲区域。这样的 DMZ 保护模式，在目前大多数中小型网络中应用广泛，其结构如图 2-60 所示。

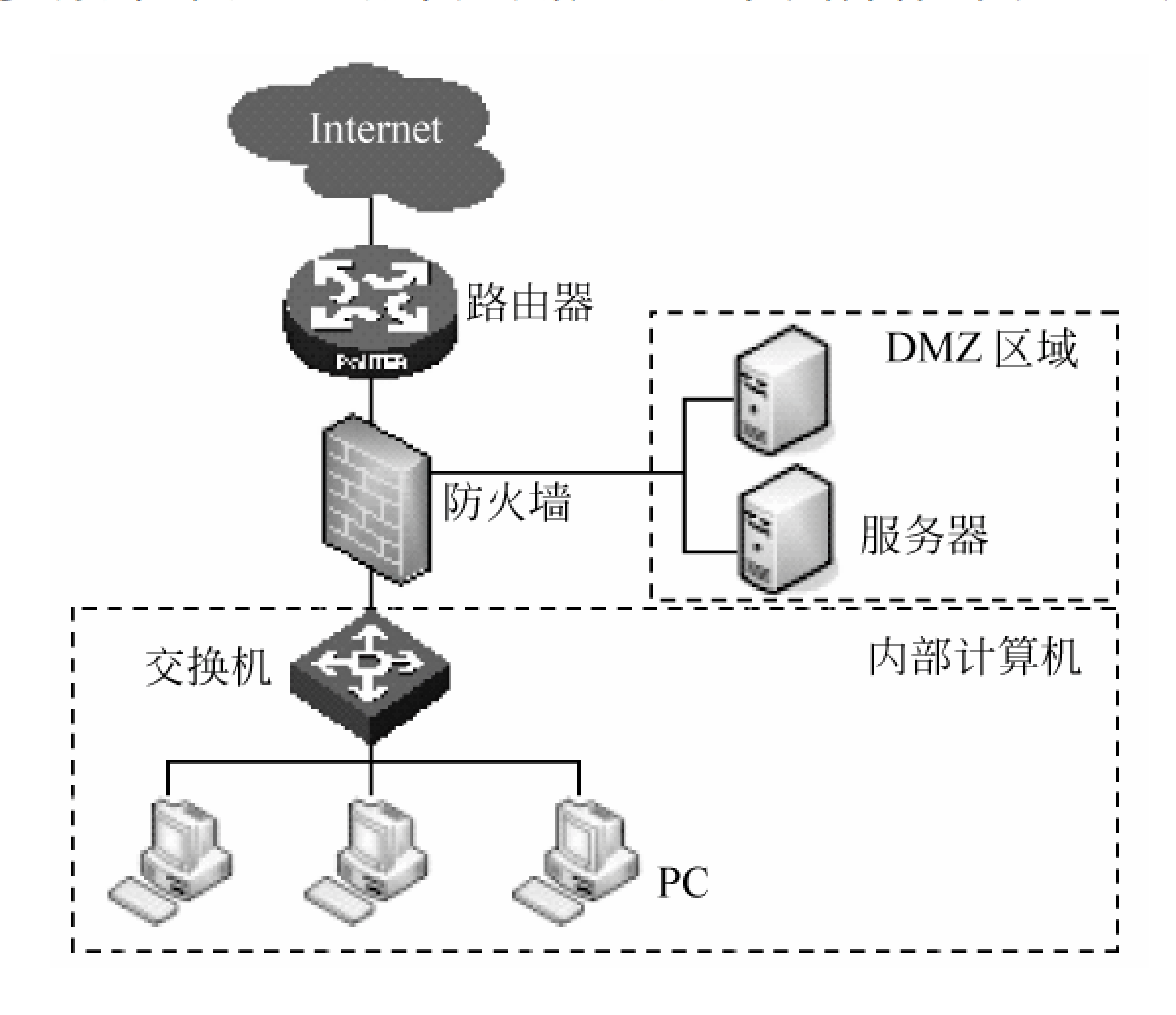


图 2-60　单防火墙构建 DMZ 保护模式

4．双防火墙构建 DMZ 保护模式

该结构中，包括外部防火墙和内部防火墙，外部防火墙主要用于构建和保护 DMZ 区域，而内部防火墙则专门用户内网防护，同时能够解决 DMZ 区主机与内网终端之间的安

全通信。双防火墙结构下，内部网络则处于防火墙的双层保护之下，更增强了内网的安全性。该结构如图 2-61 所示。

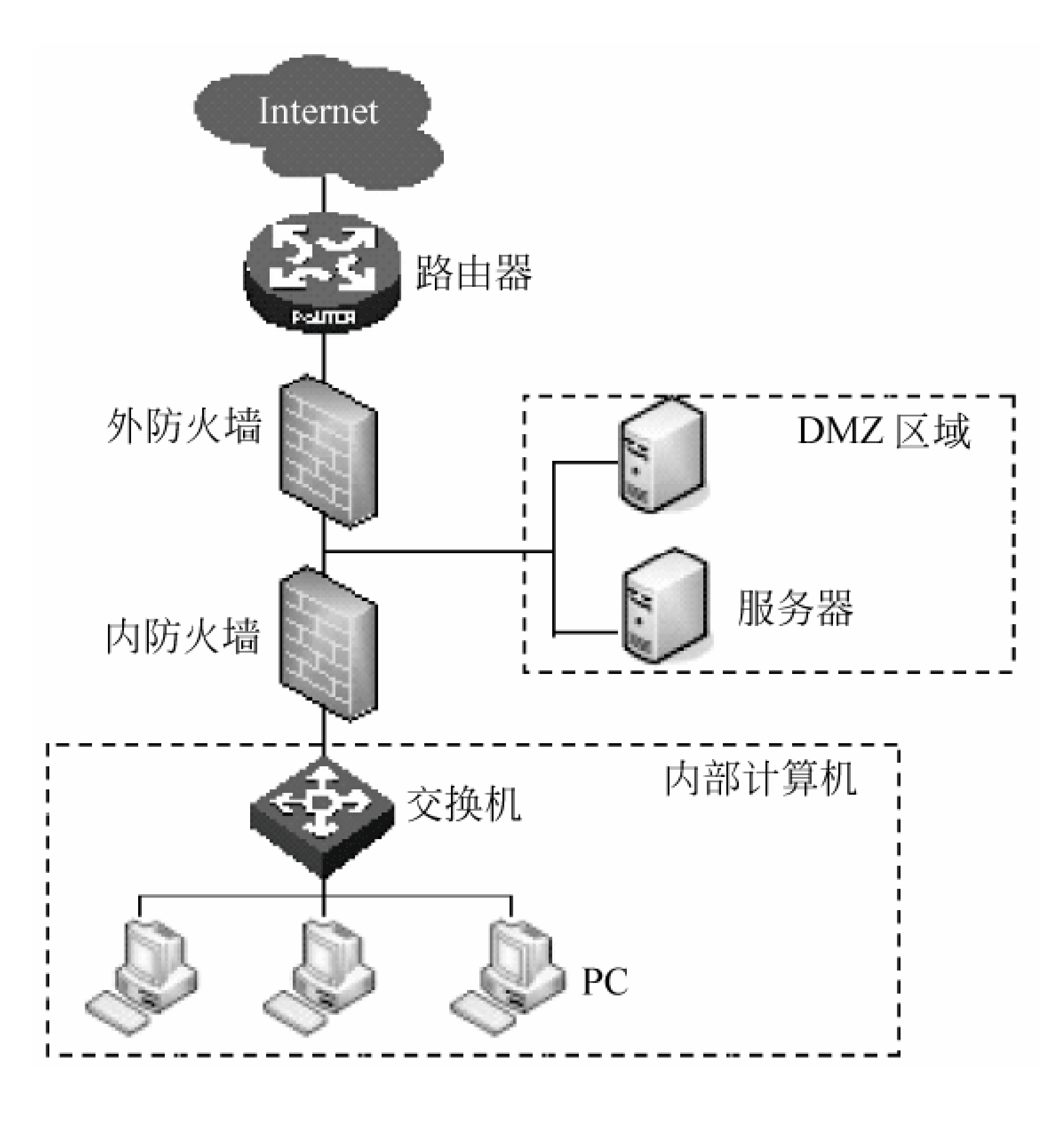


图 2-61　双防火墙构建 DMZ 保护模式

2.5 服务器介绍

服务器是为了满足更高的稳定性、可靠性和运算能力的计算机。服务器与个人计算机最大的不同在于，服务器是面向多用户同时提供服务，而个人计算机则是满足个人需求即可。同时，服务器要求 24 小时不停机的提供服务，且需运行稳定、数据吞吐率量大、包含支撑大型服务程序的后台进程等。特别是在特殊行业和重要企业中，如在银行、电信、金融等行业，服务器在并发处理能力、稳定性、安全性方面都提供了重要的支撑服务。

服务器设备广泛地应用在中型、大型企业中。而在小型企业中，服务器的数量较少，通常包含邮件服务器、Web 服务器、视频服务器等，能够满足服务需求即可。

2.5.1 服务器的分类

按照服务器的外形进行分类，可分为塔式、机架式、刀片式三种类型。

塔式服务器：与常见的 PC 台式机外形相似，但由于包含多个硬盘接口，通常其体型较大，各种不同品牌的塔式服务器，其外形尺寸各不相同，如图 2-62 所示。



图 2-62　塔式服务器

机架式服务器：机架式服务器用于满足企业密集式的部署，具有统一的宽度标准，通常为 19 英寸（19 英寸=48.26cm），用于放置在 19 英寸宽的标准机架中，其高度与路由器、交换机一样，用 U 进行描述。机架式服务器相比塔式服务器更易于管理和维护，且节约空间，布线也清晰整齐，如图 2-63 所示。



图 2-63　机架式服务器

刀片式服务器：按照其字面意思即很容易理解，刀片服务器就是一块块可插拔的母板，每一块母版就是一台单独的服务器，该类服务器占用空间更小，易于扩展且成本也更低，适用于特殊的行业或高密度的环境。可以将多块刀片式服务器组合为服务器集群，以提供更强的性能，如图 2-64 所示。



图 2-64　刀片服务器

按照服务器所提供服务的不同，可分为以下几种：

文件服务器：用于网络用户访问、共享、管理、并行操作等文件应用的服务器，如 Windows 系统下的文件服务器功能。

Web 服务器：用于发布 Web 网站的服务器，提供发布服务的程序，如 Apache、Tomcat、IIS 等。

杀毒服务器：主要用于网络版杀毒软件中服务端程序的安装，可集中控制和管理客户端杀毒程序，易于病毒库统一升级和网络病毒的查杀，例如瑞星杀毒网络版。

邮件服务器：用于实现电子邮件的接收和发送功能，常见邮件服务程序如 Exchange Server、Send Mail 等。

数据库服务器：专门用于存储数据的服务器，例如 Oracle、SQL Serve、MySQL 等。

2.5.2 服务器与个人计算机的差异

在硬件结构上，服务器设备与个人计算机相似，同样包括 CPU 处理器、内存、硬盘、主板、电源等组件，但服务器更侧重于处理能力、安全性、可扩展性等方面。以下从硬件和软件方面，分别介绍服务器与个人计算机的差异。

服务方式不同：个人用计算机是直接面用用户提供服务，而服务器通常是通过网络向用户提供公用服务，且能够同时处理多用户请求。

CPU 的不同：服务器通常采用多路 CPU 组成多处理器系统。多路即提供物理上的多个 CPU，以提高计算和处理能力。而个人计算机通常采用多核技术，即在一块 CPU 上集成了多个处理器核心。当然，随着个人计算机的迅速发展，也提供了对多 CPU 的支持。

硬盘的不同：目前主流的个人计算机使用 SATA 硬盘。而服务器通常使用三类硬盘，包括 SATA 硬盘、SCSI 硬盘以及 SAS 硬盘。相比普通硬盘，服务器硬盘有速度快、可靠性高、支持热插拔等优势，且服务器使用硬盘时，通常使用大容量的多块磁盘组成磁盘阵列，提高数据的存储速度和安全性。

内存的不同：服务器内存与普通内存在外观上无明显差别，但在功能方面，服务器内存增加了校验和自动纠错的能力，具有更高的稳定性和可靠性，服务器内存和个人计算机内存之间不可以混用。

操作系统的不同：个人计算机通常使用界面友好、多媒体功能较为丰富的操作系统，如 Windows XP、Windows 7 等，这些操作系统在功能方面省略了用于支撑大型服务程序的进程。而服务器通常使用 Unix、Linux 系统，或者专为服务器所开发的 Windows Server 系列。当然，这些操作系统具备兼容性，可任意安装在个人计算机或服务器中。

电源的不同：通常服务器会使用冗余电源系统，即电源系统由多个电源模块所组成，其中部分电源模块损坏，仍不会影响设备的运行，其目的是提高系统的稳定性。

注意：服务器和个人计算机的区分主要是看提供了怎样的服务，一台普通的低性能计算机只要能够提供应用（如 Web 服务、邮箱服务），那么该计算机同样也是服务器。

2.5.3 服务器磁盘阵列技术介绍

磁盘阵列技术就是将多个硬盘（最少两块），通过软件或硬件的结合技术，组成大容量、稳定性和安全性高的磁盘集合。该技术称为 RAID（Redundant Arrays of Independent Disks，廉价冗余磁盘阵列）。

RAID 技术经过不断的发展，现在已经包括 RAID 0 至 RAID 6 共 7 种基本的 RAID 模式。同时，在这些基础模式的基础上进行组合，形成了更多模式，如 RAID 10（RAID 0 和 RAID 1 的结合）、RAID 50（RAID 0 和 RAID 5 的结合）、RAID 6（RAID 0 和 RAID 6 的结合）等。

磁盘阵列技术包含众多优势，包括支持自动检测故障硬盘、重建损坏磁盘资料、热插拔和硬盘扩容、数据冗余和容错等。

RAID 技术可通过软件方式或硬件方式实现。软件方式即通过操作系统提供的磁盘阵列管理技术实现。在 Windows Server 版本中，即提供了磁盘阵列功能，可将若干接入系统的磁盘连接为盘阵。但软件方式，将占有较多的硬件资源，包括磁盘子系统的资源。

而硬件 RAID 方式，是通过专门的阵列卡实现盘阵功能的。该方式下，将阵列的处理都交给阵列卡处理，减少了对其他硬件资源的占用。目前，RAID 技术通常以硬件方式实现。较为常见的 RAID 卡有 SATA RAID、Fibre RAID、SCSI RAID、IDE RAID 及 SAS RAID 卡。例如 SCSI 接口的 RAID 如图 2-65 所示。

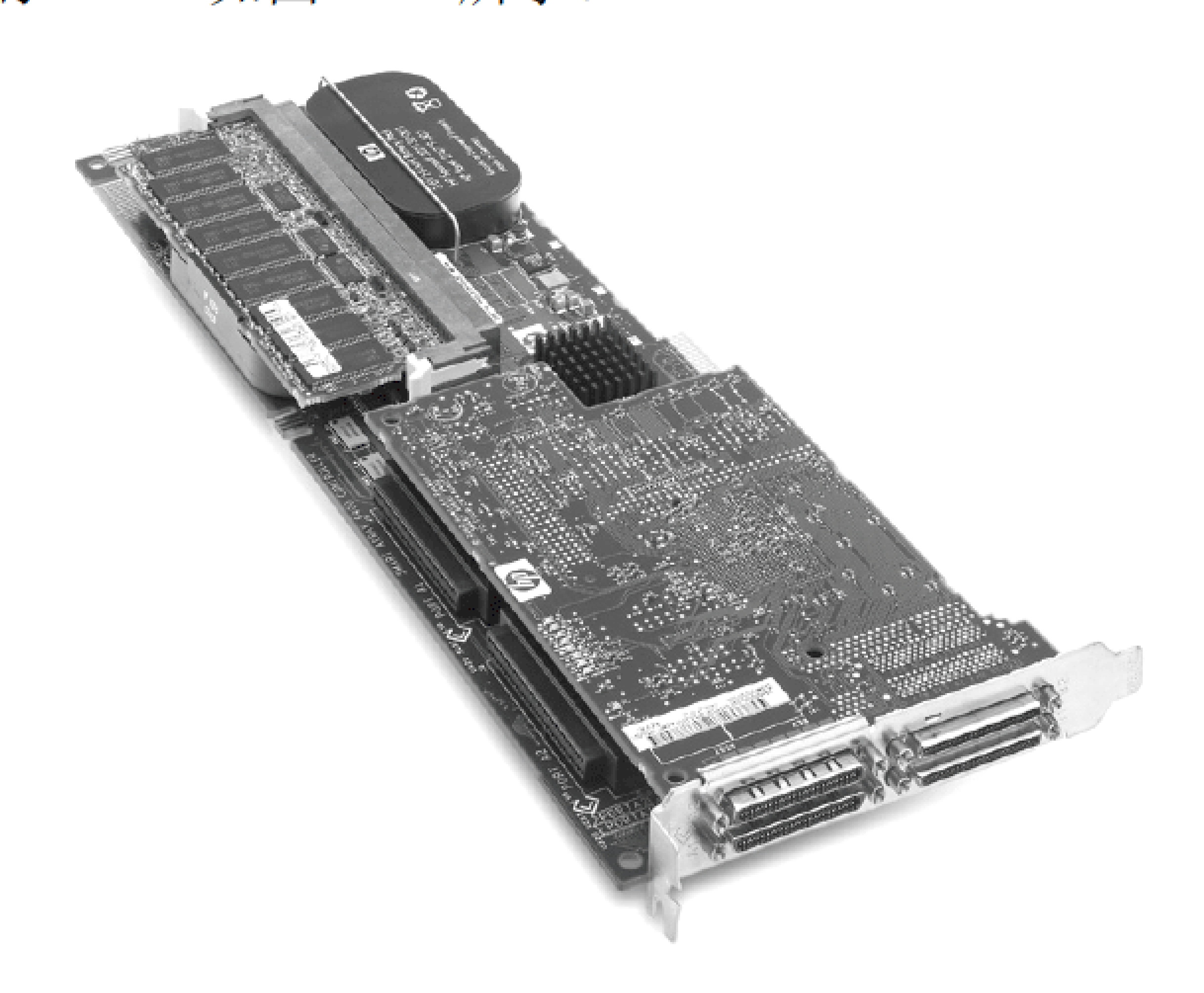


图 2-65　SCSI 接口的 RAID 卡示例

2.5.4　各类 RAID 技术介绍

目前应用较为广泛的磁阵技术包括 RAID 0、RAID 1、RAID 0＋1、RAID 5 及 RAID 50，而 RAID 2、RAID 3、RAID 4 已经被逐步淘汰。

1. RAID 0

RAID 0 技术又称为数据分块存储技术。在存储数据时，将数据分成若干大小相同的数据块，并同时写入每个磁盘中，所以 RAID 0 还有另一个称呼，即将数据条带化（Stripping）存储。该方式的最大优势在于扩展了磁盘的容量和存取速度，有 N 块硬盘组成了 RAID 0 阵列，则磁盘空间和存取速率均扩大了 N 倍。该方式的缺点在于可靠性极差，当其中一块磁盘发生故障时，将导致整个阵列无法使用。RAID 0 的结构如图 2-66 所示。

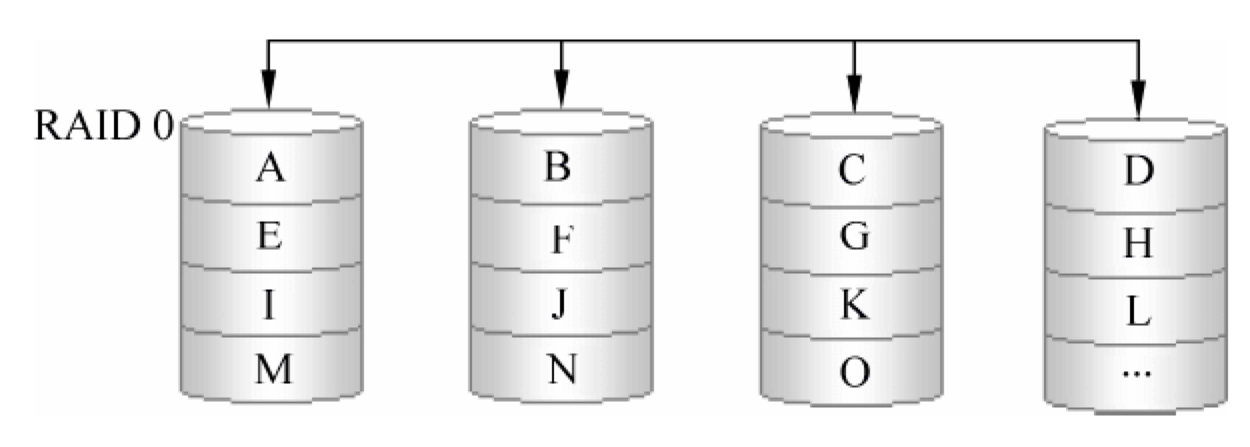


图 2-66　RAID 0 盘阵结构

2. RAID 1

RAID 1 技术又称为镜像。每一个工作硬盘都有一个镜像盘，在写入数据到磁盘时，将数据同时完整地写入到工作盘和镜像盘中。简单的理解，也就是将工作盘中的数据完全复制到镜像盘，使磁盘中存储的数据内容完全相同并互为热备。当其中一个磁盘出现故障时，另一个盘将接替读写工作。在更换故障磁盘后，经过数据的同步，再次形成互为热备的磁盘组合。该方式下，磁盘的容量将变为原来的一半，但其数据的安全性极高。RAID 1 结构如图 2-67 所示。

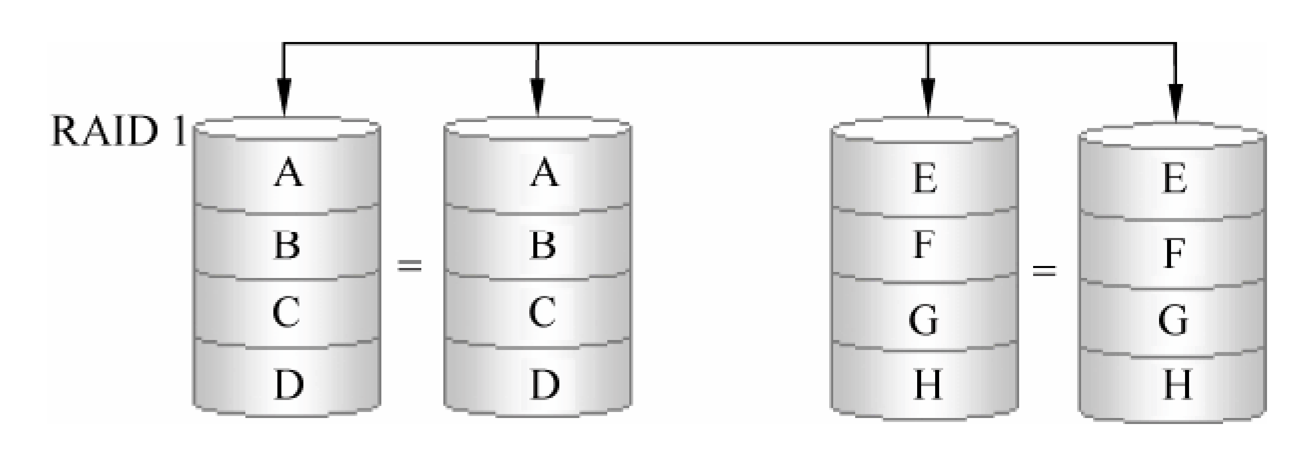


图 2-67　RAID 1 盘阵结构

3. RAID 0+1

该方式即 RAID 10，同时具备了 RAID 0 读写速度快和 RAID 1 安全性高的优点。RAID 10 至少需要 4 块硬盘才能够实现。该方式将 4 块硬盘分为两组，每一组的两块硬盘组成 RAID 0 方式，两组 RAID 0 又通过 RAID 1 方式互为镜像，使得读写性能和数据安全性都得以兼顾。但 RAID 10 的成本较大，且磁盘空间利用率较低，并不是科学和经济的方式。RAID 0+1 结构如图 2-68 所示。

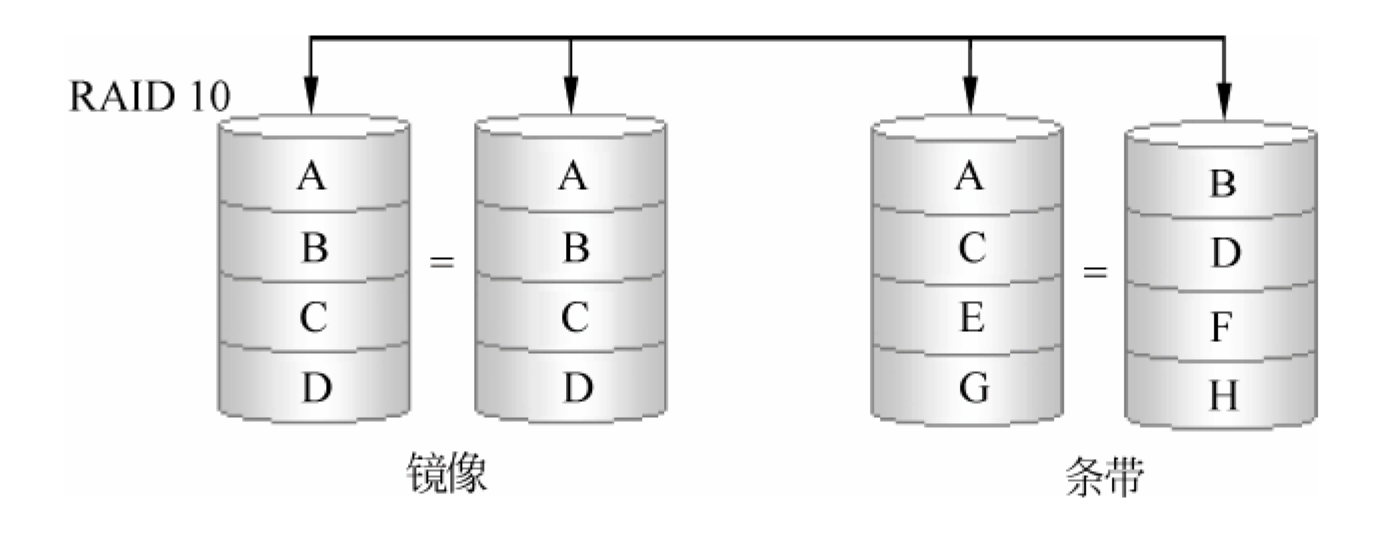


图 2-68　RAID 10 盘阵结构

4. RAID 3

RAID 3 增加了奇偶校验技术，并使用一块单独的磁盘存储校验信息，而剩下的磁盘采用 RAID 0 的数据分块存储方式。RAID 3 具备容错的功能，也增加了额外的时间和资源开销。当其中一个磁盘出现故障时，需要重新建立校验信息，更换故障磁盘后，还需重新按数据块重建数据内容。但如果损坏的磁盘是校验盘，那么将导致数据的丢失和阵列的不可用，所以 RAID 3 方式应用较少。RAID 3 结构如图 2-69 所示。

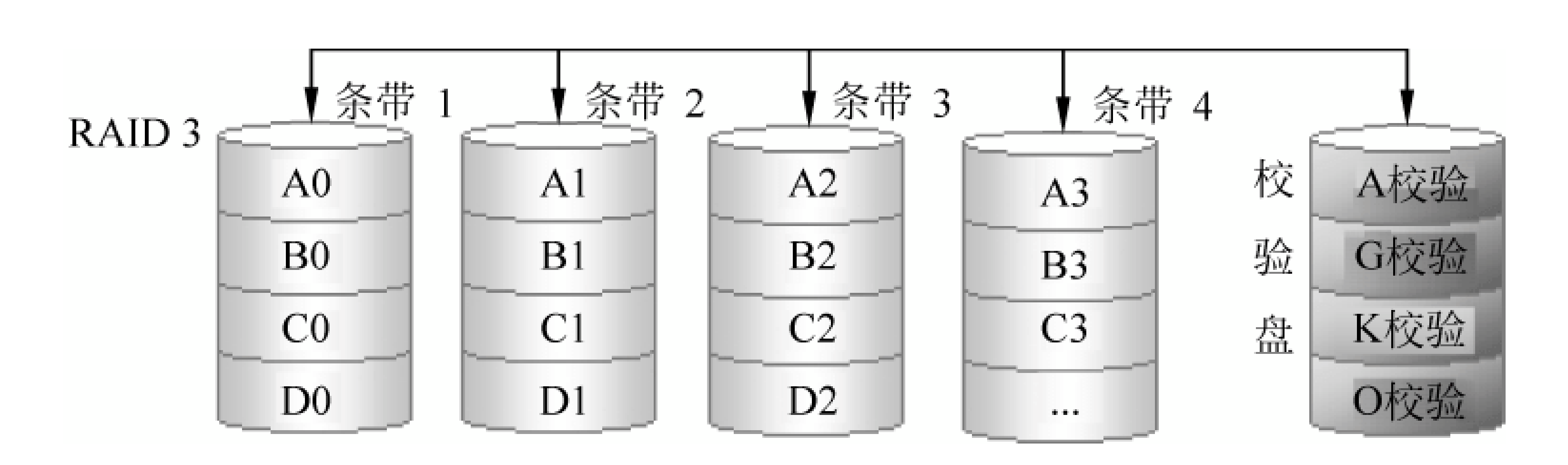


图 2-69　RAID 3 盘阵结构

5. RAID 4

RAID 4 方式与 RAID 3 相似，同样采用校验盘和 RAID 0 方式的结合。不同之处在于，RAID 3 使用字节或位存储数据，而 RAID 4 以块或扇区为存储单位。那么，在 RAID 4 方式下在进行数据存取时，只需操作一个数据盘和校验盘即可，而不像 RAID 3 的方式操作任何数据都需要牵动全组盘阵。但该方式下，校验盘同样会成为系统的瓶颈，所以 RAID 4 也较少使用。RAID 4 结构如图 2-70 所示。

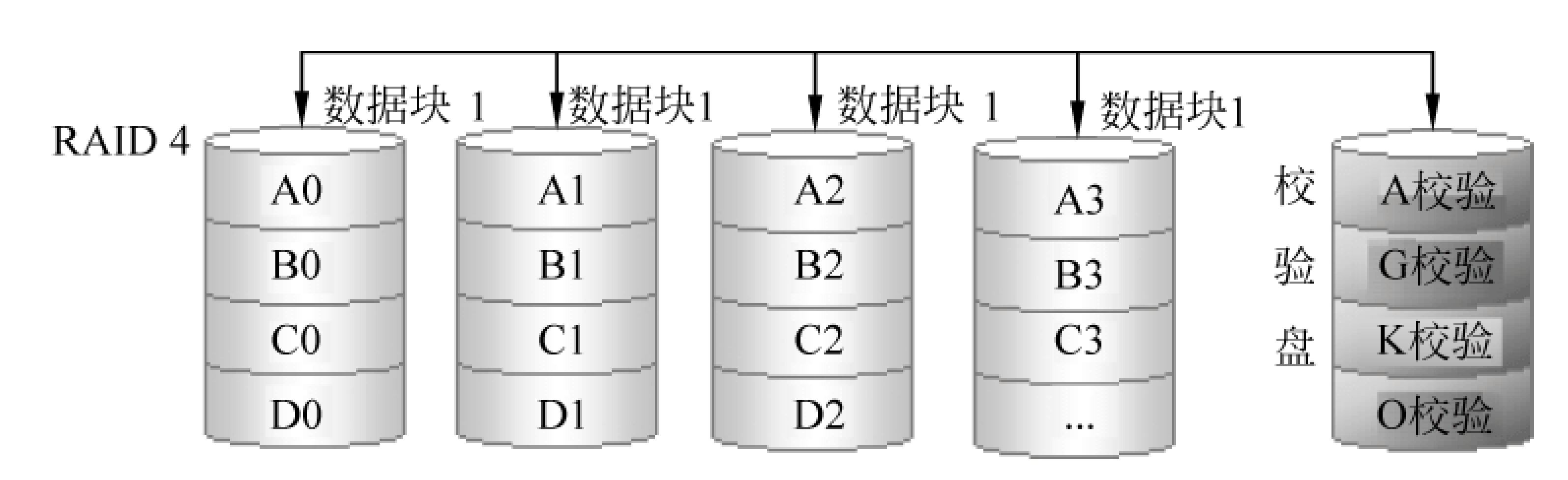


图 2-70　RAID 4 盘阵结构

6. RAID 5

RAID 5 是目前应用较为广泛的磁盘阵列技术，要实现该方式至少需要 3 块磁盘。RAID 5 同样采用了奇偶校验技术，但并不单独提供校验磁盘，而是将校验数据分布到每一块磁盘中，数据存储则采用 RAID 0 的分块存储方式。该方式具有磁盘空间利用率高（N 块磁盘可包含 N-1 的容量）、数据读写速度快、安全性高的优势，是 RAID 3、RAID 4 的完全替代者。RAID 5 结构如图 2-71 所示。

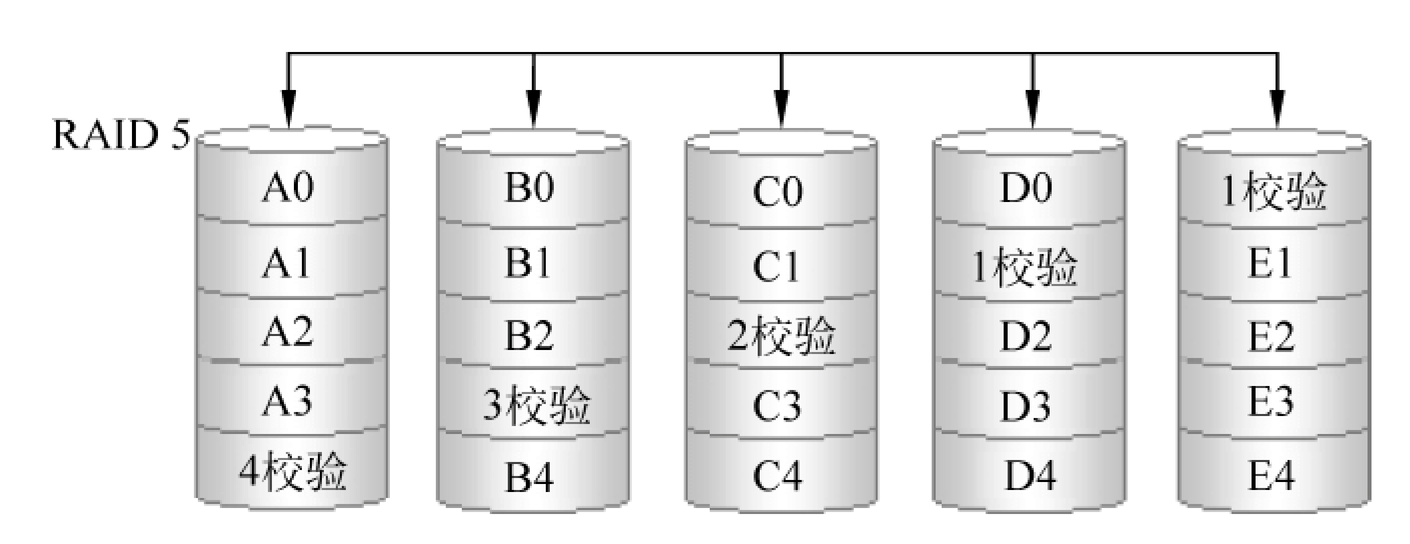


图 2-71　RAID 5 盘阵结构

7. RAID 6

RAID 6 采用了与 RAID 5 相似的分割存储方式，并在 RAID 5 技术的基础上进行了扩

展。RAID 5只包含一组奇偶校验技术，而RAID 6包含两组，在对数据块进行分层校验基础上，还提供总体数据的校验，因而具备更高的容错能力。其最大的特点是能够同时支持两个磁盘出现故障，以防止数据的丢失。要实现RAID 6至少需要4块硬盘。其结构如图2-72所示。

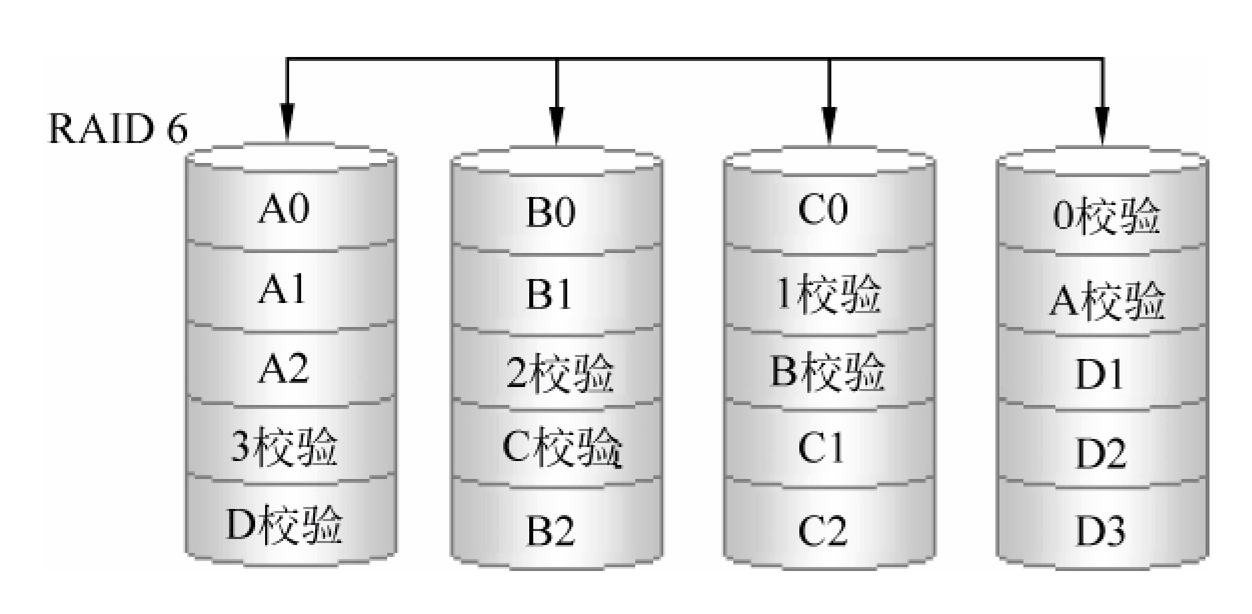


图2-72　RAID 6盘阵结构

8. RAID 7简介

RAID 7被称为存储计算机操作系统，它不仅仅是一种磁盘阵列技术，而是发展成为了一种存储操作系统，用于控制RAID 7盘阵中的数据操作和传输。RAID 7可不占用CPU资源，完全独立于主机运行，使磁盘读写性能达到最佳。而且，当一个磁盘出现故障时，还可自动执行故障恢复以及数据重建过程。RAID 7是目前理论上性能最高的RAID 模式，同时也是费用最贵的。

9. RAID50简介

RAID 50技术结合了RAID 0和RAID 5的优势，通常也被称为镜像阵列条带技术，要实现RAID 50至少要求6块磁盘，其中每3块磁盘组成一组RAID 5模式，两组RAID 5模式又组成RAID 0模式。数据写入磁盘时，采用的是RAID 0的条带存储方式，在同一时间写入多块磁盘。同时，采用了RAID 5的校验技术，将校验数据写入到各个磁盘中，以保证数据的安全。

2.6 本章小结

本章主要介绍了计算机网络中的常见网络设备，包括网卡、交换机、路由器、防火墙和服务器设备等。还介绍了与这些设备相关的管理、操作、配置等应用知识，以帮助网络管理员加深对这些设备的认识和理解。本章所涉及的知识点同样是网络管理员必须理解和熟悉的基础知识。

第 3 章　网络协议的概念及应用

网络协议在网络中的地位异常重要，它是网络互联、通信的规范和标准。网络管理员在日常维护过程中，会碰到大量的各类网络协议。虽然并不需要了解协议的具体内容，但仍然应熟知各类协议的定义和用途及协议所服务的对象和应用，以便于解决网络故障，分析和优化网络。

在日常网络管理和维护中，将接触到多种协议。例如，用于检查网络是否畅通，需要用到最简单的 ICMP 和 IP 协议；在邮件服务器出现故障时，需要检查 SMTP 或 POP3 等邮件服务协议是否正常运行；而在网络监测时，需要用到 SNMP 协议，包括该协议的安装、开启和配置，以及如何通过 SNMP 协议获取所需的网络信息。

本章首先简介 OSI 七层模型和 TCP/IP 模型，然后分别介绍各类常见协议的概念、发展和实例应用。具体的协议包括：HTTP、FTP、Telnet、ICMP、ARP、TCP/IP、DNS、IPX/SPX、SNMP、SMTP、POP3。本章除介绍协议的基本概念，还将通过其具体应用以加深理解。

3.1　网络模型的概念

网络协议就是计算机网络中所有设备之间进行通信的规则和标准。通信包括了建立连接、数据传输、交换等内容。在网络终端实现通信时，源主机和目的主机需要遵循相同的规则，也就是遵循相同的协议。否则有一方将无法识别另一方的“语言”，而导致通信异常或中断。

网络协议类似于交通系统中的路牌标识，只有遵循统一的指示标识，才能够保证目的地的正确可达。如果不明白指示牌的意义，那么就有可能失去方向。

3.1.1　OSI 七层协议模型

ISO（国际标准化组织）和 CCITT（国际电报电话咨询委员会）共同出版了 OSI（开放系统互联七层模型）。该模型定义了网络通信过程中，从用户提出应用请求到最终数据通过物理链路传送到目的地的整个过程。其中还涵盖了编码、加密、压缩、路由寻址、存储转发、数据封装、多路复用、数据分割重组、差错控制、流量控制、拥塞控制等技术和协议的定义。

OSI 七层模型的结构如图 3-1 所示。

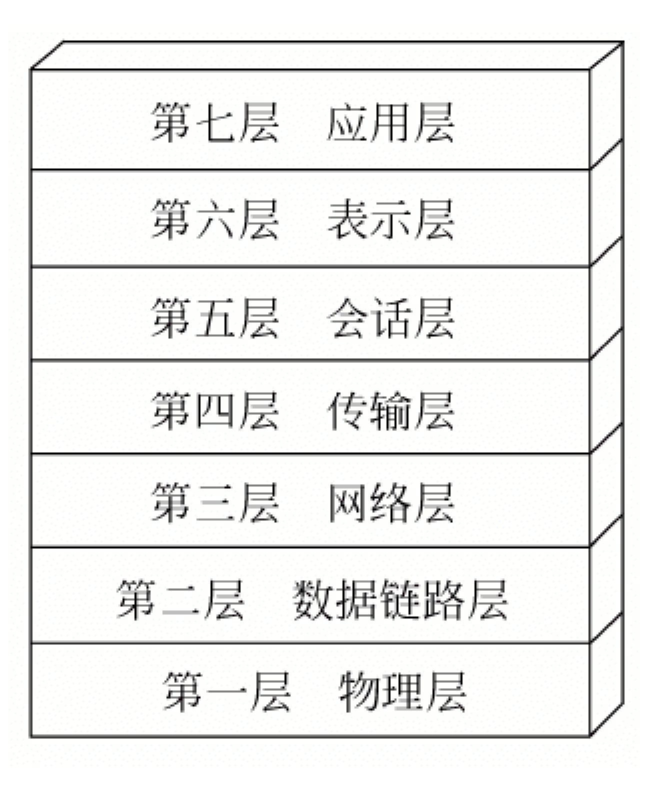


图 3-1　OSI 七层模型

OSI 七层模型中，各层的定义极其相关的协议见表 3.1。

表 3.1　OSI 七层模型中各层的定义和相关协议

协　议　层	定义和描述	相 关 协 议
物理层（Physical Layer）	定义了传输数据的物理链路特性，包括机械特性、接口规范、物理介质等。其主要功能是提供传输的物理链接，并规定数据以比特流（Bit）的方式传送	本层典型的规范有 RS-232、V35、RJ45 等
数据链路层（Data Link Layer）	为通信实体双方建立数据链路，将比特流数据包封装为帧（Frame）进行传输，并提供流量控制、差错控制手段使得物理链路变成无差错的数据链路	PPP（点到点协议）、STP（生成树协议）、帧中继等
网络层（Network Layer）	定义了将数据封装为数据包（Packet）进行传输，主要完成为数据包寻找最佳路径和转发，并提供了拥塞控制、网络互联等功能	IP、RIP（路由信息协议）、OSPF（开放最短路径协议）等协议
传输层（Transport Layer）	管理数据包实现端到端的可靠传输，提供数据包分段和重组、差错恢复等功能	TCP、UDP、SPX（序列分组交换协议）
会话层（Session Layer）	完成不同设备之间会话的建立、管理和释放，区分不同的会话，确保会话之间的同步，以及管理数据的交换	
表示层（Presentation Layer）	定义数据的编码和解码、压缩和解压缩、加密和解密等功能，通过这些数据转换确保源数据在目的端的正常识别	
应用层（Application Layer）	定义了网络之间通过程序实现通信和数据传输的接口和方式，用户可通过程序实现与网络的直接对话	Telnet、FTP、HTTP、SNMP 等服务协议

3.1.2　TCP/IP 协议模型

TCP/IP（Transfer Control Protocol/Internet Protocol，传输控制/网际协议）是互联网的基础和核心协议。Internet 就是在 TCP/IP 协议的基础上发展起来的。该协议具备良好的兼

容性、可靠性和可扩展性，可支持不同结构不同类型的网络，例如电信网、互联网、工业控制网、物联网、局域网、广域网等。

TCP/IP 协议是由一组网络通信协议组成，通常称之为 TCP/IP 协议族。TCP/IP 协议族的发展和变革，直接影响和制约着下一代互联网的发展。该协议模型相比 OSI 七层模型更为实用和简洁，共分为四个层次，如图 3-2 所示。

第四层　应用层
第三层　传输层
第二层　网际层
第一层　网络接口层

图 3-2　TCP/IP 协议模型

TCP/IP 协议的四层结构中，各层的定义和相关协议见表 3.2。

表 3.2　TCP/IP 协议模型的各层定义及协议

协　议　层	定义和描述	相 关 协 议
应用层（Application Layer）	定义了与网络相关的程序与其他程序建立连接的接口、协议等规范。该层直接提供基于软件应用的协议	HTTP、Telnet、FTP、SNMP、DNS、SMTP 等协议
传输层（Transport Layer）	负责网络主机之间的传输会话管理，提供相关的数据通信和传输服务，以确保数据的可达	TCP（面向连接传输协议）、UDP（面向无连接协议）和 RTP（音视频等实时传送协议）
网际层（Internet Layer）	TCP/IP 模型中的核心层，负责数据的存储转发、寻址和路由等功能，同时还负责异构网络互联、网络差错控制、拥塞控制等	IP、ICMP、ARP（地址解析协议）、RARP（反向地址解析协议）
网络接口层（Link Layer）	定义了数据包通过传输介质在实际网络中进行传输的协议。	以太网、令牌环、FDDI、X.25、帧中继等

3.1.3　OSI 和 TCP/IP 模型的关系和对比

该两种模型按照其层次所对应的协议进行归纳，可形成大致的对应关系，如图 3-3 所示。

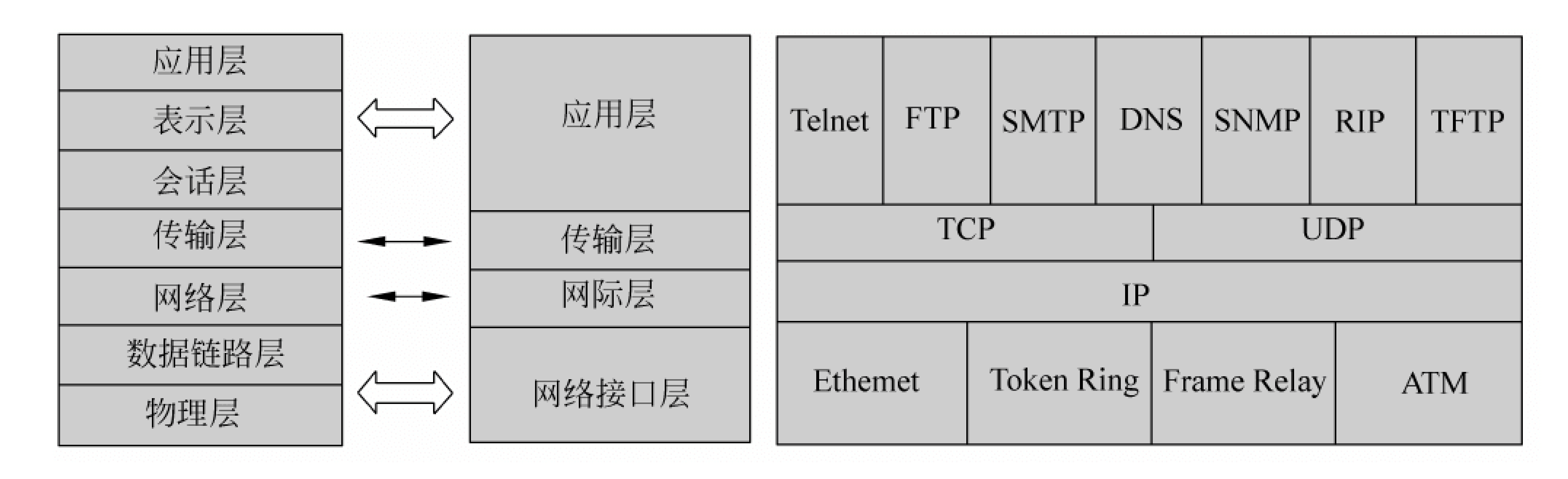


图 3-3　OSI 和 TCP/IP 模型的对应关系

1．OSI 与 TCP/IP 模型的相似之处

- 两种模型功能大体相似，都定义了网络通信的整体过程，以及通信过程中所涉及的控制技术。

- ❑ 两种模型均采用了层次结构，且都是按照功能划分层次。
- ❑ 两种模型中传输层以上的层次均是面向具体应用的控制层次。

2．OSI 与 TCP/IP 模型的不同之处

- ❑ OSI 模型存在严格的层次关系，即数据的传输必须严格经过逐层的处理，每个层只能接收来自下一层所提供的服务，而 TCP/IP 协议可以跨越层次使用更低层提供的服务，更能够提高协议的效率。
- ❑ TCP/IP 模型能够支持不同结构类型的网络，而 OSI 七层模型主要是面向数据网络将不同系统进行互联的模型。
- ❑ TCP/IP 模型对面向连接和无连接的服务提供了同样的支持力度，而 OSI 模型更多地偏重面向连接的服务。
- ❑ TCP/IP 模型具有更高的网络管理能力，而 OSI 七层模型在该方面功能较弱。

3.2 各类网络协议详解

3.2.1 ICMP 协议

ICMP（Internet Control Message Protocol，Internet 控制信息协议）是最常见的网络协议。它是 TCP/IP 协议族中的一个子协议，可通过该协议在网络主机与主机之间、主机与网络设备之间发送控制消息的数据包，用于测试网络的连通性和目的主机的可达性等。

ICMP 协议最常见的应用就是 Windows 系统的 Ping 命令和 Tracert 命令，以及 Linux\Unix 系统的 Traceroute 命令。Ping 命令即发送测试网络连通性的数据包，Tracert 和 Traceroute 则用于跟踪探测数据包的传递路径。Ping 命令在之前的章节中已经进行了详细介绍，此处主要介绍 Tracert 和 Traceroute 命令的应用，另外介绍一个路由跟踪命令 Pathping。

1．Tracert 命令

基本语法：Tracert 目标主机名或 IP 地址

例如，使用该命令检查数据包到达 Web 站点 www.sina.com.cn 所经过的路径。在命令提示符中输入该命令（如图 3-4 所示），从图 3-4 中可看出，局域网内数据包到达指定 Web 站点所经历的路由节点一共是 12 个。

Tracert 命令是非常实用的命令。那么，在什么情况下会使用该命令呢？例如，在局域网无法访问互联网时，可使用该命令 Tracert 任意一个 Web 站点。正常状态下，数据包应该是经过楼层接入交换到达核心交换机，然后被发送至路由器和防火墙，之后被转发至互联网路由器，数据包每经过一个 IP 地址，都会收到回送的确认。此时可查看，数据包是在

经过哪一个 IP 地址时停止了传送，此时便可定位故障点。

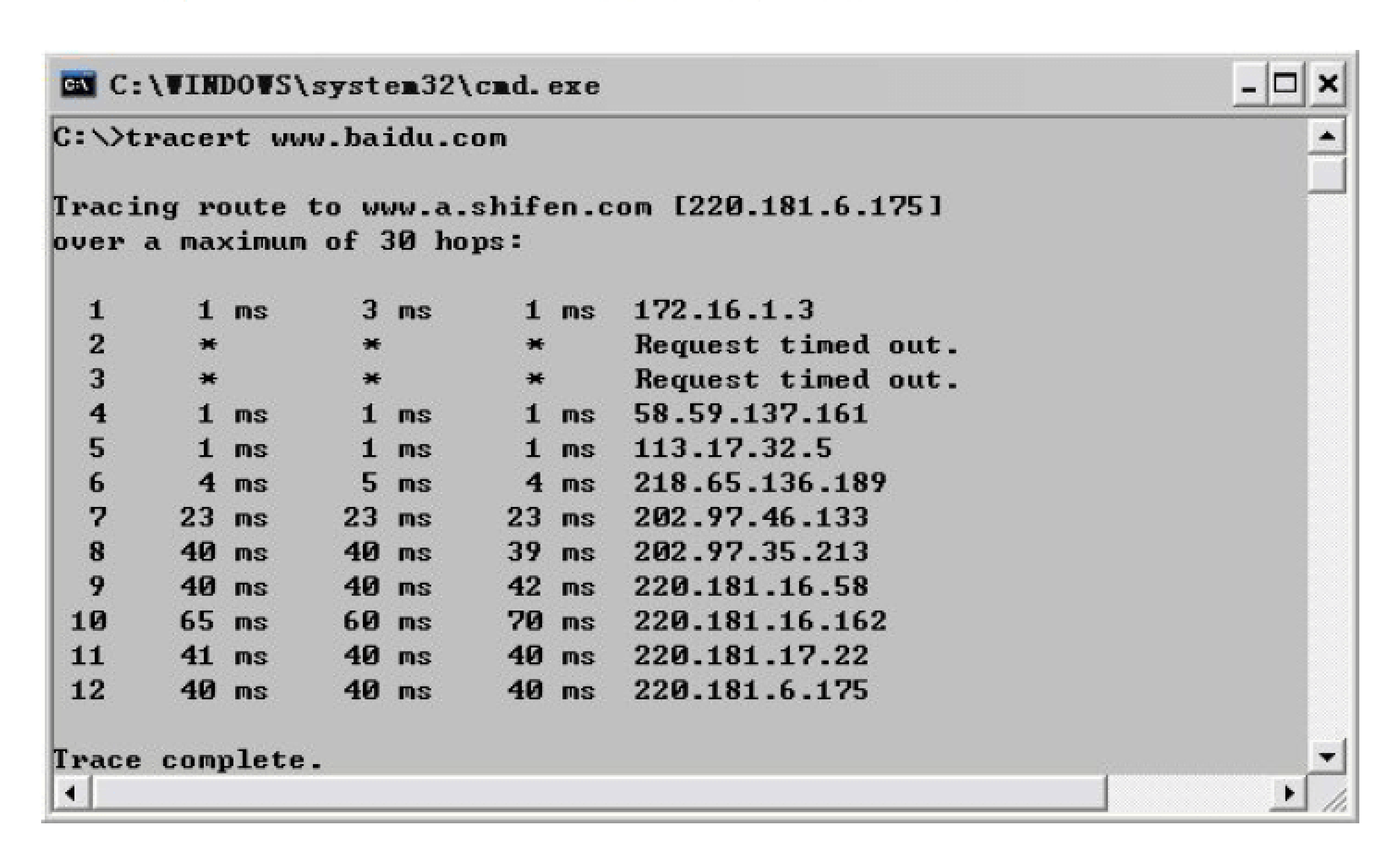


图 3-4　Tracert 命令的执行结果

2. Traceroute 命令

基本语法：Traceroute 目标主机名或 IP 地址

Traceroute 是 Linux 操作系统中的路由跟踪命令。同样执行该命令探测数据包到达 Web 站点 www.sina.com.cn 所经过的路径。该命令执行后如图 3-5 所示。

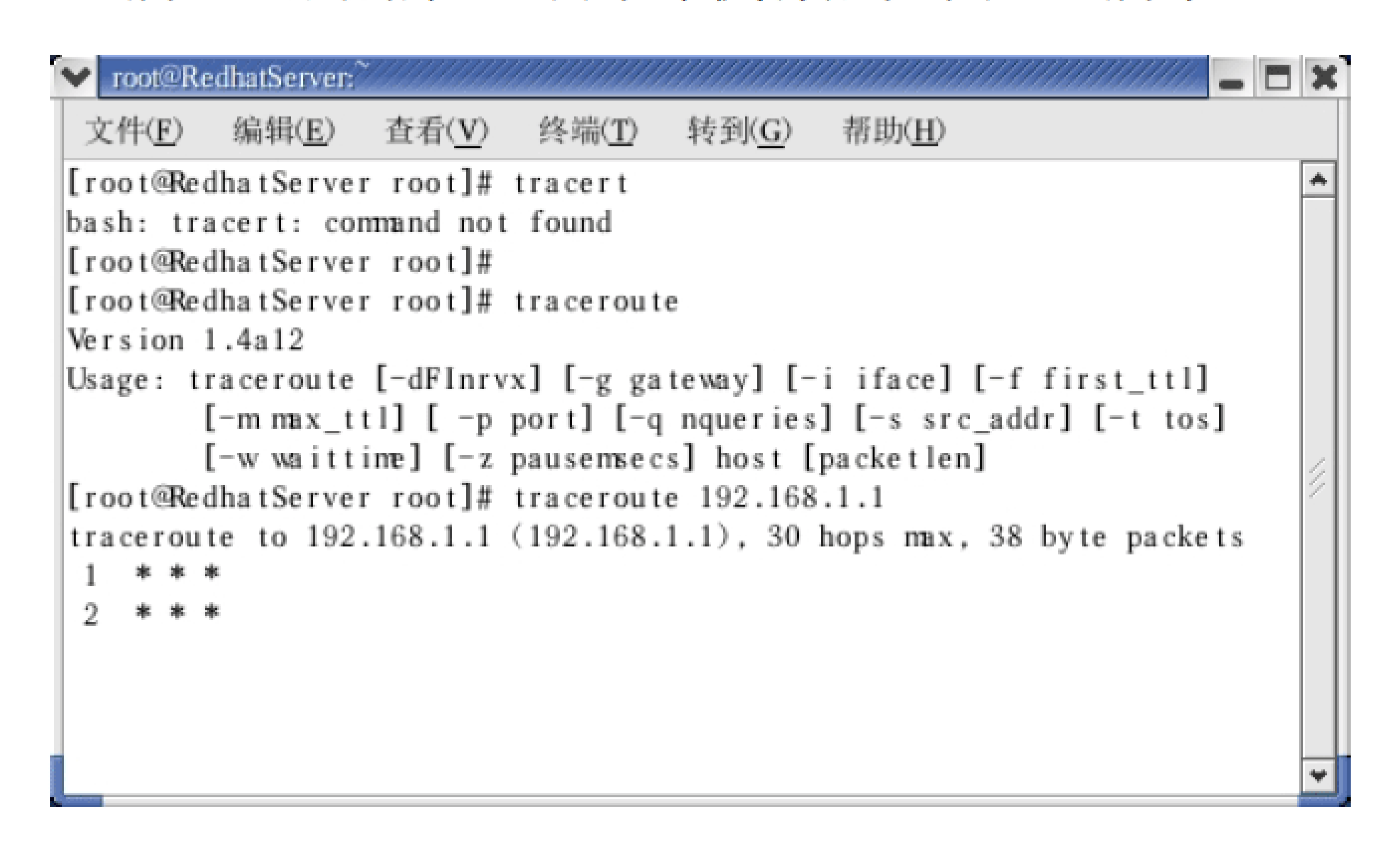


图 3-5　Traceroute 命令的执行结果

值得注意的是，Traceroute 命令发送的是 UDP 类型的数据包。如需发送 ICMP 类型的数据包，可在该命令后添加参数-I，发送 TCP 类型的数据包，添加参数-T。

注意：Tracert 和 Traceroute 的区别如下：

（1）Tracert 是 Windows 系统的命令，而 Traceroute 是 Linux\Unix 中使用的命令；

（2）Tracert 是发送 ICMP 请求回复确认的数据包，而 Traceroute 是向目的地址发送 UDP 类型的数据包。

3. Pathping 命令

基本语法：Pathping 域名或 IP 地址

该命令同样是路由跟踪命令，它是 Ping 和 Tracert 命令的结合。该命令通过定期向传输路径中的节点发送数据包，并计算返回的数据包，以统计丢包的情况。该命令可用于诊断导致网络故障或延迟的节点，在 Windows 命令提示符下执行，如图 3-6 所示。

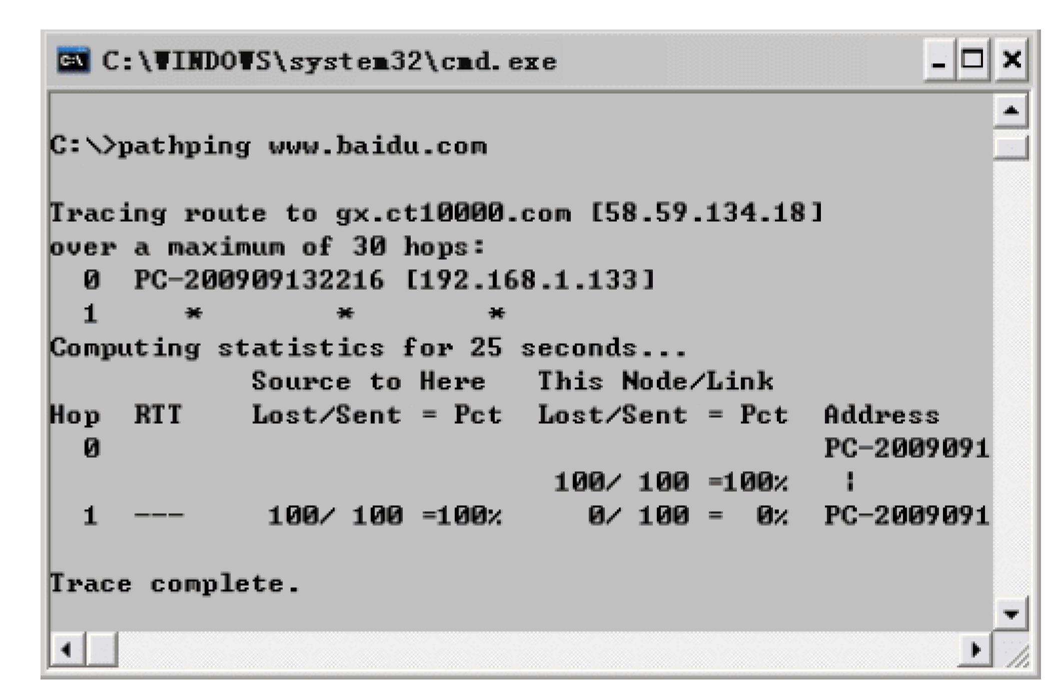


图 3-6 Pathping 命令执行结果

3.2.2 HTTP 和 HTTPS 协议

HTTP（Hyper Text Transport Protocol，超文本传输协议）是互联网中应用最为广泛的协议，所有的 Web 服务都需要遵循该协议。该协议主要用于实现客户端浏览器与 Web 服务器端之间的通信和会话。其定义了用户访问互联网服务器资源的标准，包括访问服务器上传文件、下载内容、运行服务程序等。通俗地讲，HTTP 协议就是用户用于访问 Web 网站的标准，该协议默认使用 TCP 80 端口。

HTTPS（Secure Hypertext Transfer Protocol，安全超文本传输协议）是以 HTTP 协议为基础发展而成。相比 HTTP 协议，HTTPS 采用了数据加密和压缩的技术，提高了传输数据的安全性，被广泛应用在对数据安全性要求较高的通信，例如银行、邮箱、在线支付等方面。

HTTP 协议和 HTTPS 协议的区别如下：

- HTTP 协议是明文传输，而 HTTPS 采用了压缩、加密、身份认证等技术传输。
- HTTP 协议使用 80 端口，而 HTTPS 使用 443 端口。
- HTTP 协议效率高，而 HTTPS 由于加密和压缩的消耗，其处理效率和性能较低。
- HTTPS 协议需要申请证书，而免费的证书较少，通常需付费使用。

1. Http 协议发展历程

HTTP 协议是一种典型的客户端\服务器应用模式，最早于 1990 年提出，发展至今，一共经历了 3 个版本，HTTP0.9、HTTP1.0 和 HTTP1.1。

HTTP0.9 版本：已经淘汰，该版本是一种简单的请求和回答协议，无法显示和处理图片及其他格式的数据。

HTTP1.0 版本：1.0 版本在 0.9 版本的基础上有了较大发展，能够支持和处理多种格式的 Web 数据，例如图片、音频和视频。该版本的特点是无连接性，即当服务器与客户端之间只保持短暂的会话，浏览器的每次请求都需要新建一个 TCP 连接，服务器在处理完请求后立即断开连接，所以建立和关闭连接增加了额外的开销，但 HTTP1.0 的第 6 版仍是目前应用较为广泛的版本。

HTTP1.1 版本：与 1.0 版本相比，HTTP1.1 版本具有更强的可靠性和功能性，且支持持久性连接，即客户端建立一次连接，就能够完成多次请求和响应，减少了重复建立和关闭连接的时间。除此之外，1.1 版本还提供了身份认证、缓存处理、错误通知和状态管理

等高级功能。

如需要在 Windows 系统中查看所使用 HTTP 协议版本，可在 Internet Explorer 浏览器上打开快捷菜单，并选择【属性】|【高级】页面，在第一个设置项中即可看到 HTTP 的版本，如图 3-7 所示。

2. 协议应用和示例

在 Web 服务器中存放的网页文件都是 HTML（超文本信息）文件格式。客户端需要访问这些 Web 页面，就需要通过 HTTP 协议来传递和翻译超文本信息。客户端用户首先在浏览器输入一个网址或选择某个超链接，浏览器就向 Web 服务器的 IP 地址发送了一个 HTTP 请求，Web 服务器在接收请求后，通过 HTTP 协议将 Web 站点中的网页代码提取并翻译成人性化的网页界面，之后回传给客户端浏览器。

目前，比较流行的 Windows 系统的浏览器有 Internet Explorer、Opera、Firefox 等，而在 Linux 系统中较流行的浏览器是 Lynx。

HTTP 协议的网站很多，只需要在浏览器中输入网站地址即可。而使用 HTTPS 协议的网站相对较少。访问 HTTPS 协议网站，将弹出安全警报，提示使用安全证书访问。例如，在标题栏输入 https://www.gmail.com 的邮箱网址，将弹出提示框，如图 3-8 所示。

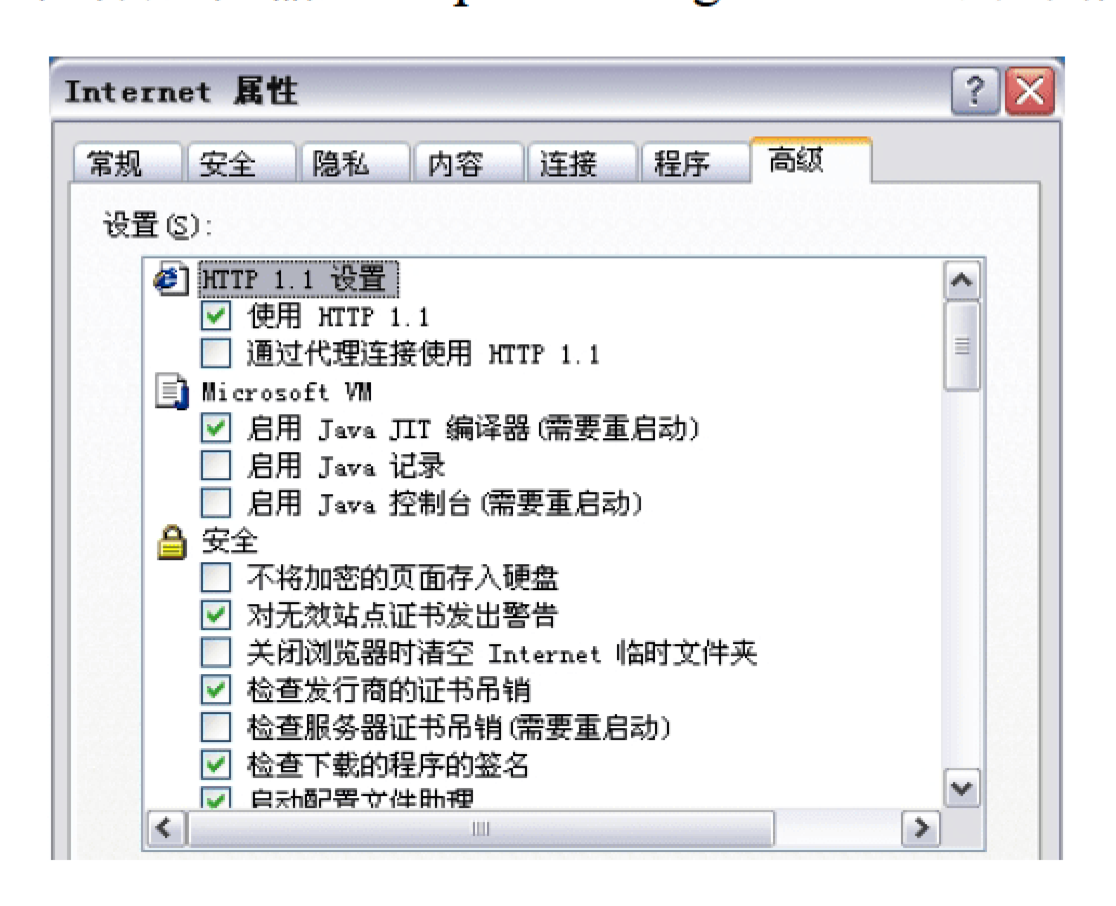


图 3-7 在 Windows 系统中查看 HTTP 协议的版本

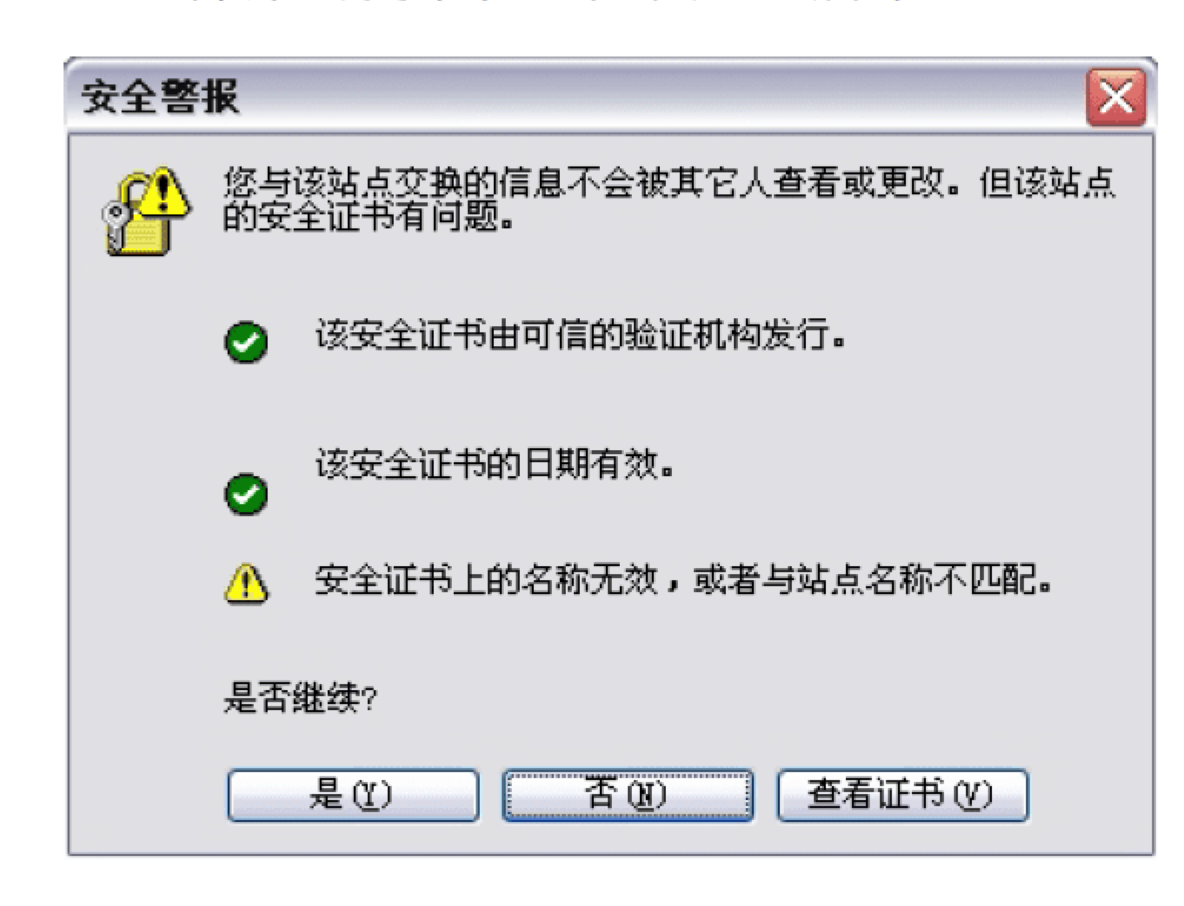


图 3-8 使用 HTTPS 协议访问网站弹出的提示框

选择【是】按钮继续访问站点，此时将使用 HTTPS 协议进行交互，将提高保证邮件传输的安全性，在标题栏中可看到 HTTPS 的连接标识，如图 3-9 所示。



图 3-9 HTTPS 协议应用

3.2.3 FTP 协议

FTP（File Transfer Protocol，文件传输协议）协议定义了计算机用户从互联网服务器上获取文件的方式。通过该协议，用户可从远程服务器中查看、下载文件。如果授权用户对远程服务器进行管理，那么还可上传文件和远程管理。

FTP 协议通常使用 20 和 21 端口，20 端口用于传输数据流，而 21 端口用于传送控制信息。

FTP 协议最早于 1971 年提出，其官方文档是 RFC 114。经过两年的发展，于 1973 年分别推出了官方文档 FRC 454 和 RFC 542。在修订的 FRC 542 版本中，确定了 FTP 协议的功能、基本模型和发展目标。

在 1985 年，官方文档 RFC 959 最终确定了 FTP 协议的标准定义，并沿用至今。

3.2.3.1 配置 Windows 系统的 FTP 服务

此处介绍在 Windows Server 2003 操作系统中，建立供局域网访问的 FTP 目录，以加深对 FTP 协议的理解。如果要建立通过互联网访问的 FTP 服务器，还需要“花生壳”等域名解析软件的配合，以及申请 FTP 域名。局域网搭建 FTP 共享服务器，配置过程介绍如下。

在 Windows Server 2003 系统中，进入控制面板，选择【添加\删除 Windows 组件】|【应用程序服务器】|【Internet 信息服务 IIS】选项，在列出的 Windows 组件中，选择【文件传输协议（FTP）服务】复选框，并安装该服务，如图 3-10 所示。

安装了 FTP 服务组件后，需确定该服务已经启动。进入控制面板，选择【管理工具】|【服务】，在服务列表中，选择 FTP Publishing Service 选项，将看到该服务的运行状态，如果服务是停止的，则将该服务启动，如图 3-11 所示。

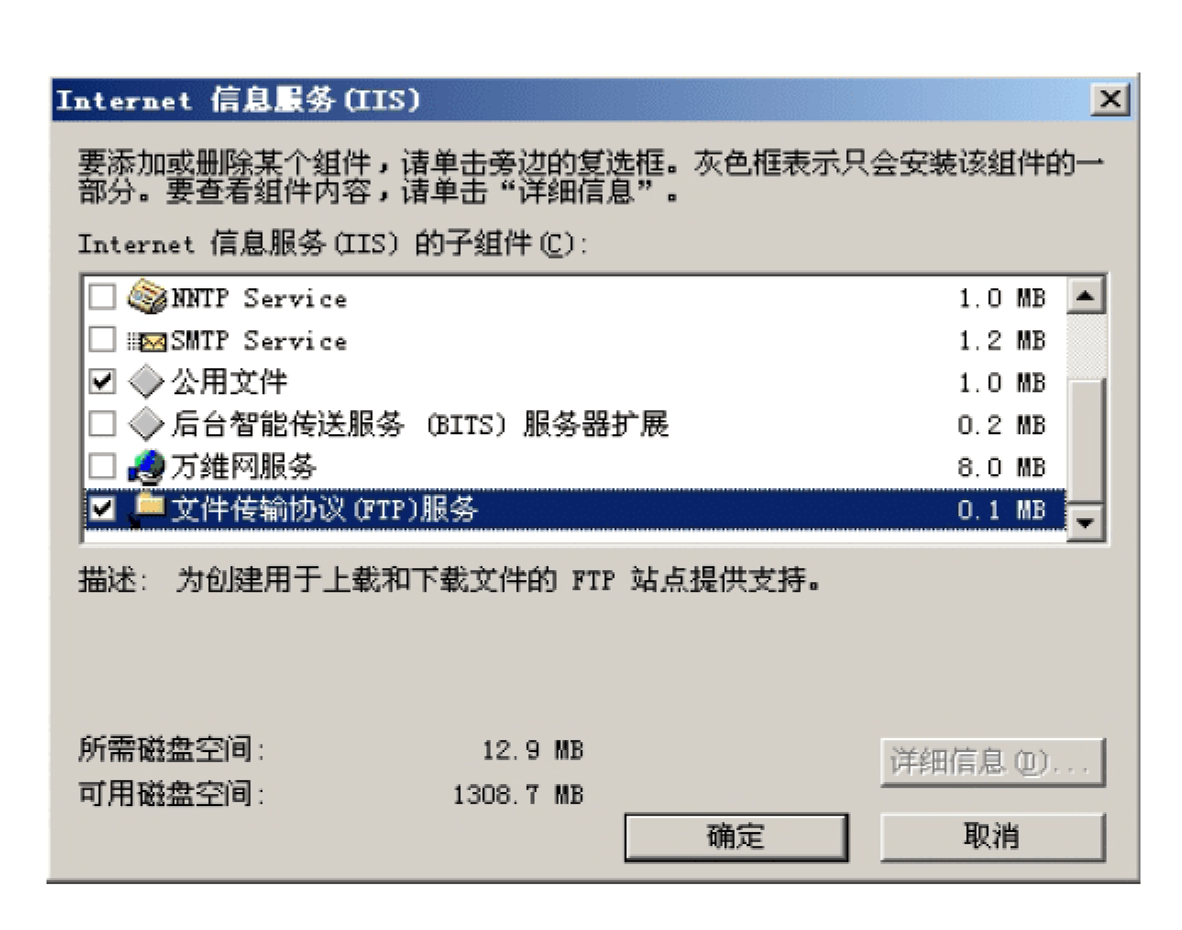


图 3-10 安装 FTP 服务组件



图 3-11 启动 Windows 系统 FTP 服务

FTP 服务开启后，需建立一个 FTP 站点供远程访问。选择开始菜单中的【程序】|【管理工具】|【Internet 信息服务器（IIS）管理器】菜单命令，在配置界面中打开【FTP 站点】选项的快捷菜单，并选择【新建】|【FTP 站点】命令，如图 3-12 所示。

在新建的 FTP 站点的配置界面中，按步骤输入该 FTP 站点的别名、IP 地址、共享的 FTP 目录、允许操作 FTP 目录的权限等，即完成了 FTP 站点的新建。其中，IP 地址设置为服务器本机地址即可，如图 3-13 所示。

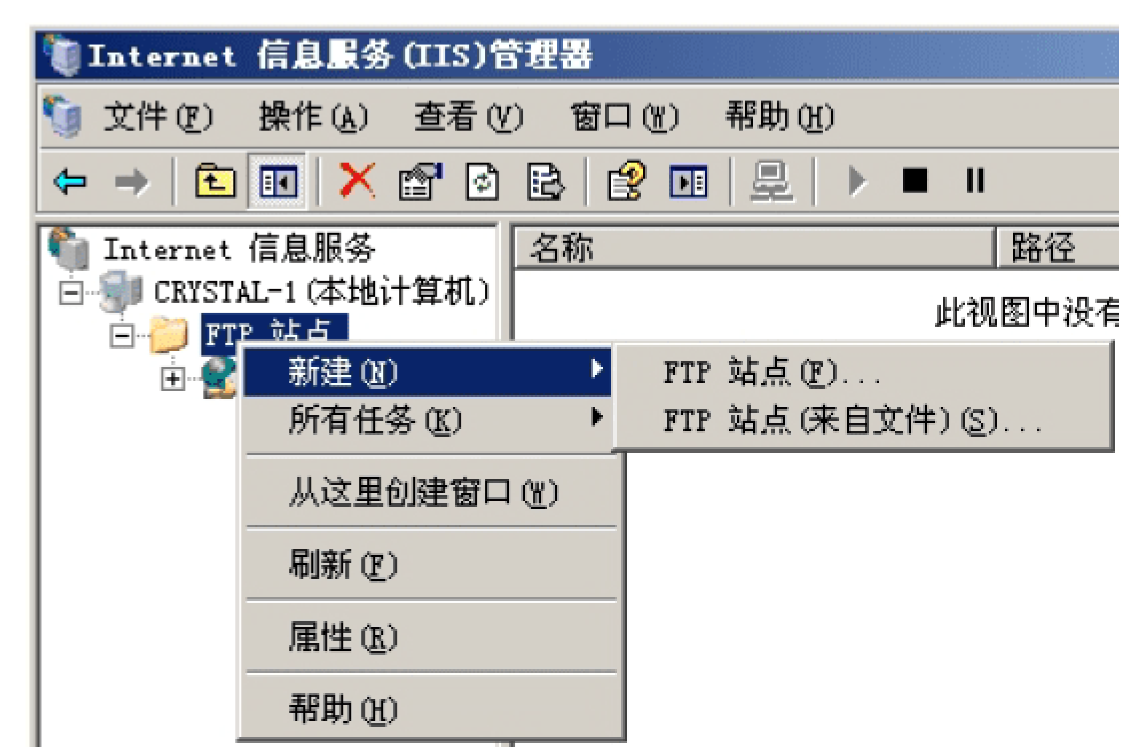


图 3-12 新建 FTP 站点

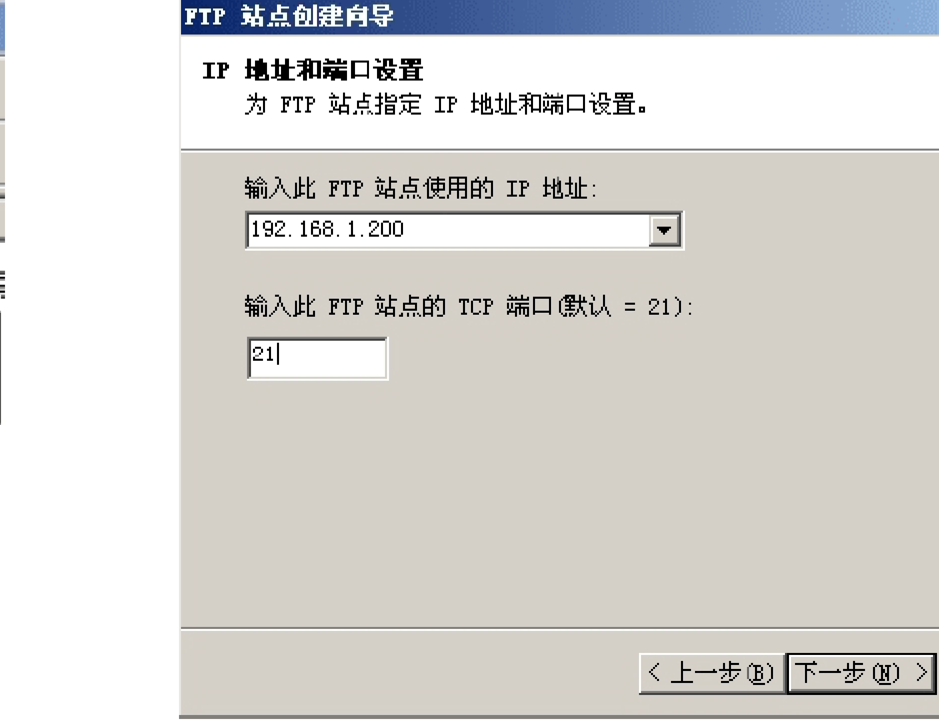


图 3-13 设置 FTP 站点的 IP 地址为本机地址

注意：（1）在新建 FTP 站点中设置了 IP 地址，那么【默认的 FTP 站点】就不能够再使用该 IP 地址。

（2）该 FTP 站点包含一个主目录，如果需要指定多个 FTP 共享目录，那么可通过建立多个虚拟目录的方式实现。

建立 FTP 站点后，需要设置其访问权限。在新建的 FTP 站点上打开快捷菜单，并选择【属性】|【安全账户】，此处如果选择【允许匿名连接】复选框，那么用户登录时不需要认证即可访问共享目录，反之则需要输入登录账号和口令，如图 3-14 所示。



图 3-14 设置是否允许匿名登录 FTP 服务器

此时，FTP 服务设置完成。可在命令提示符中通过 FTP 命令远程登录，或在 Web 页面输入该 FTP 服务器的 IP 地址访问。但使用 FTP 命令方式登录 Windows 系统，意义并不大，因为 Windows 下只提供了很少的操作命令。

此处使用 Web 页面远程登录。在客户端主机的 Web 页面中输入 FTP：//192.168.1.200，如果 FTP 服务器允许匿名登录，那么可直接查看和下载 FTP 服务器中共享的资源，否则需

输入正确的访问口令，如图 3-15 所示。

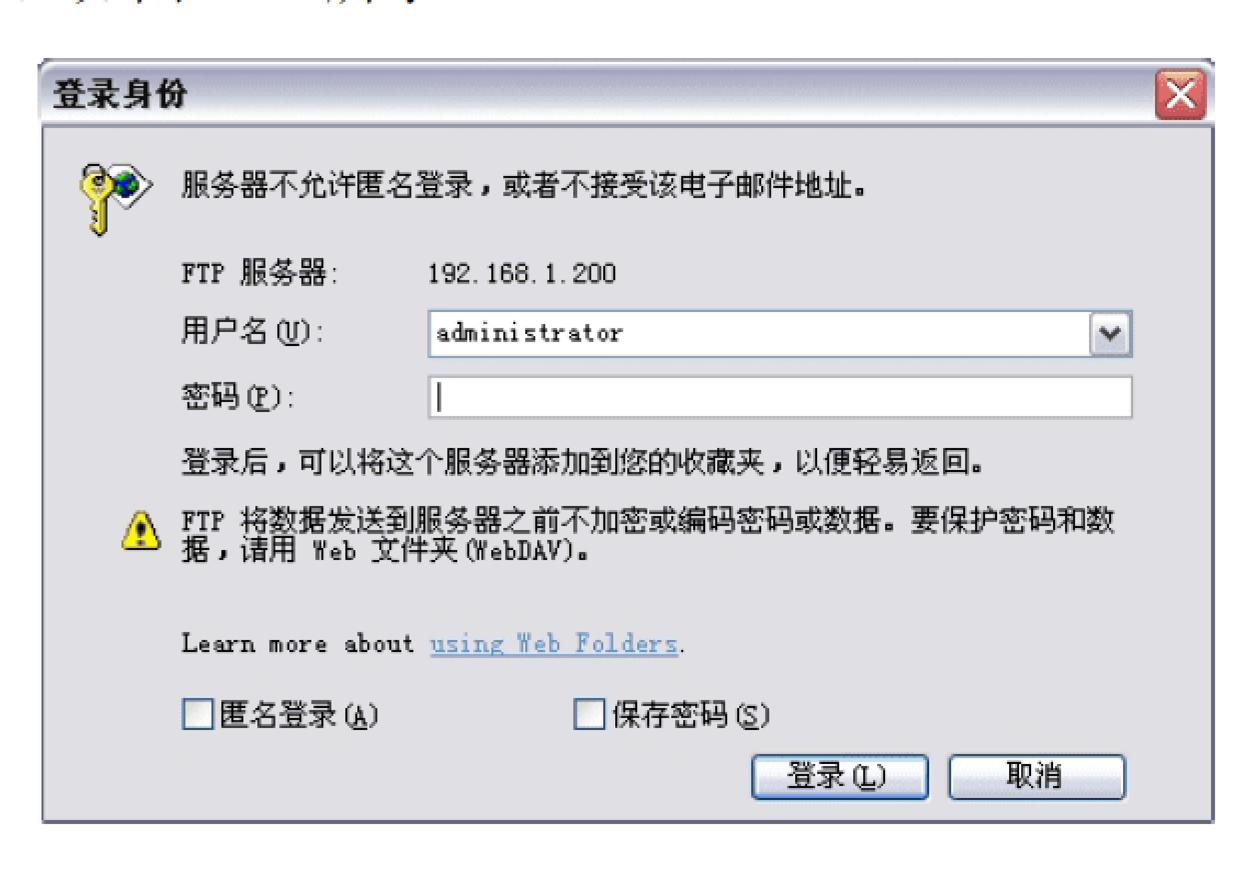


图 3-15　登录 FTP 服务器的口令认证界面

在输入正确的口令后，即可看到 FTP 站点中共享的目录和文件，如图 3-16 所示。

通过 Web 访问 FTP 服务器无法实现断点续传的功能，所以通常使用专门的 FTP 工具进行远程连接，例如 FlashFTP。在工具中，需要输入远程服务器的 IP 地址及正确的用户名和口令，即可登录到远程服务器中，如图 3-17 所示。

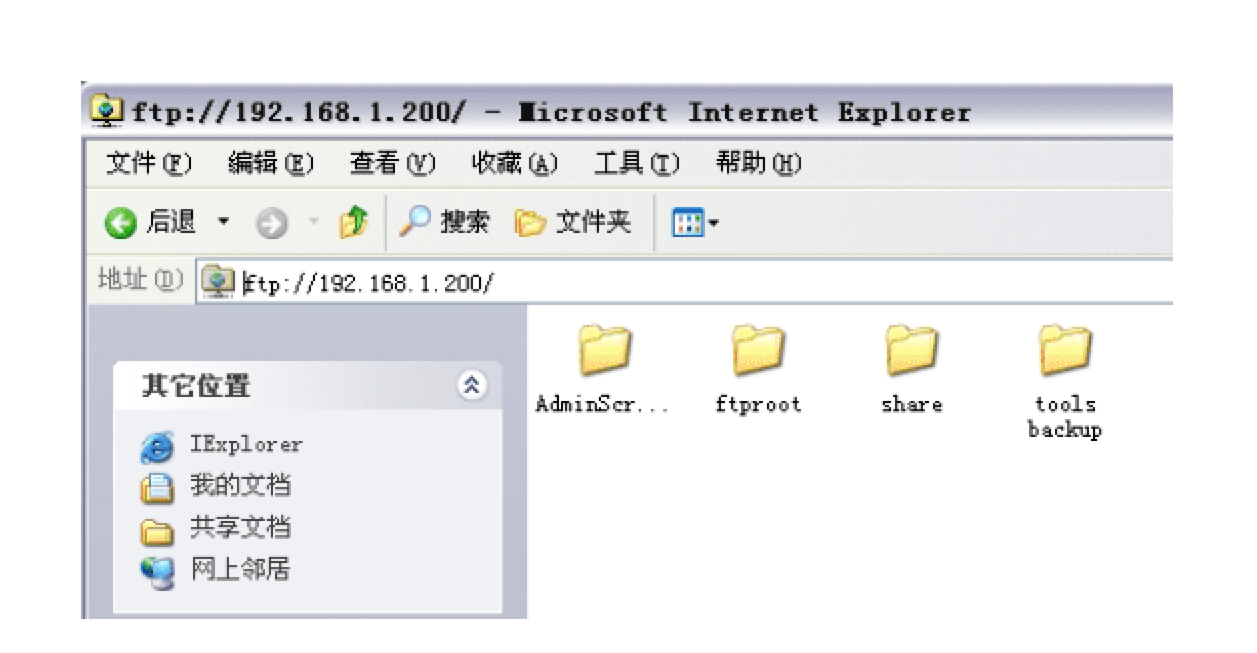


图 3-16　Web 方式登录 FTP 服务器

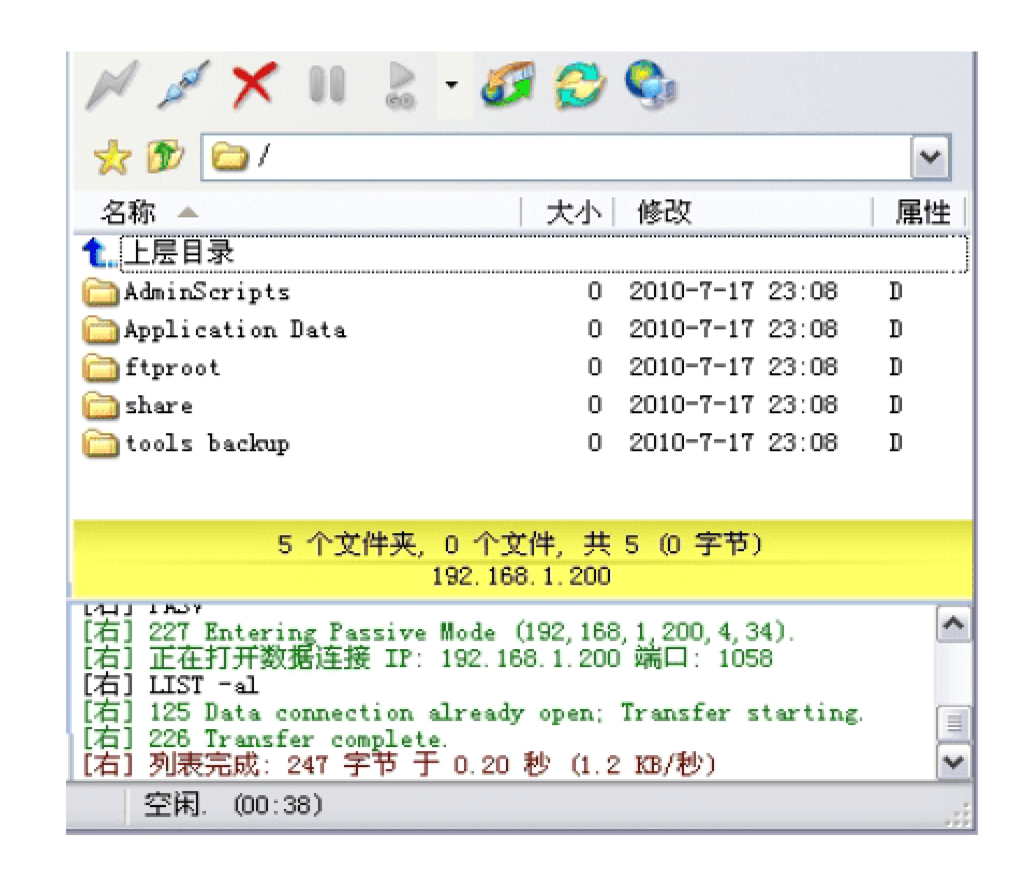


图 3-17　使用 FTP 软件登录 FTP 服务器

3.2.3.2　配置 Linux 系统的 FTP 服务

如果需要登录到 Linux 中上传或下载文件，则需要开启 Linux 中的 FTP 服务，也就是允许客户端通过 FTP 方式连接到 Linux 系统。此处以 Redhat Linux 9 为示例，配置过程如下。

（1）编辑 FTP 服务的配置文件 gssftp，在 Linux 命令行配置界面中，使用如下命令：

```
[root@RedhatServerroot]#vi /etc/xinetd.d/gssftp
```

在该文件中，找到代码行 server_args = –l –a，将–a 删除，更改为 server_args = –l。之后将代码行 disable=yes 改为 disable=no，更改后的配置文件如图 3-18 所示。

（2）修改配置文件后，需要启动 FTP 服务，使用如下命令：

```
[root@RedhatServerroot]#service vsftpd start
```

如果正常启动，将提示服务状态为[OK]。

（3）配置 Linux 允许客户端使用 root 账户通过 FTP 方式登录，编辑/etc/vsftp.ftpusers 文件，命令如下：

```
[root@RedhatServerroot]#vi /etc/vsftpd.ftpusers
```

在代码行 root 前添加符号“#”，将其注释掉。之后，编辑/etc/vsftpd.user_list，命令如下：

```
[root@RedhatServerroot]#vi /etc/vsftpd.user_list
```

同样，在代码行 root 前添加符号“#”，将其注释掉。

此时，便完成了 Linux 的系统 FTP 服务的配置。在 Windows 系统命令提示中，使用 FTP 命令，并输入登录用户名和口令后，即可登录 FTP 到服务器上，如图 3-19 所示。

```
service ftp
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/kerberos/sbin/ftpd
        server_args     = -l
        log_on_failure  += USERID
        disable         = no
}
```

图 3-18　配置 Linux 系统 FTP 服务

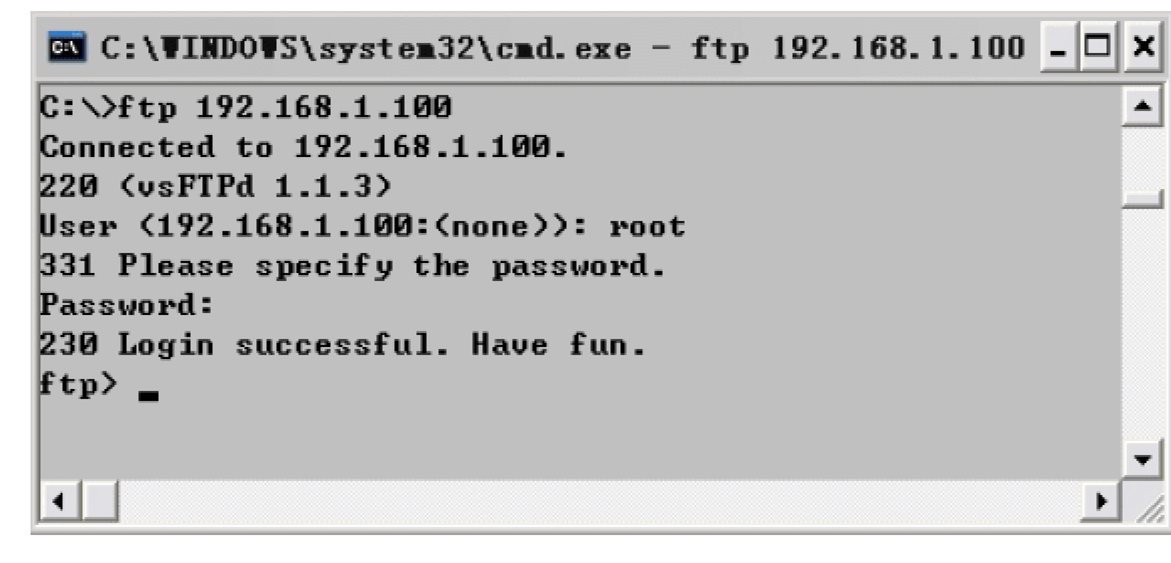


图 3-19　FTP 方式远程登录 Linux 服务器

3.2.3.3　FTP 常见命令介绍

尽管有多种 FTP 程序，可以很方便地实现数据的上传和下载。但要了解 FTP 协议，仍需熟悉其常见的命令。此处介绍通过远程连接工具 SecureCRT 登录 Redhat Linux 系统后的常用操作命令。

1．Pwd 和 Lcd 命令

- Pwd 命令：列出远程服务器端 Linux 主机中的当前目录。
- Lcd 命令：列出当前客户端 Windows 主机中的当前目录。

以上命令执行结果如图 3-20 所示。

2．Dir 和 Ls 命令

- Dir 命令：显示远程主机当前目录下文件的详细内容。
- Ls 命令：显示远程主机当前目录下的文件名列表。

Dir 命令执行结果如图 3-21 所示。

3．Get 和 Mget 命令

- Get 命令：从远程服务器下载文件，语法为 Get [文件名]。

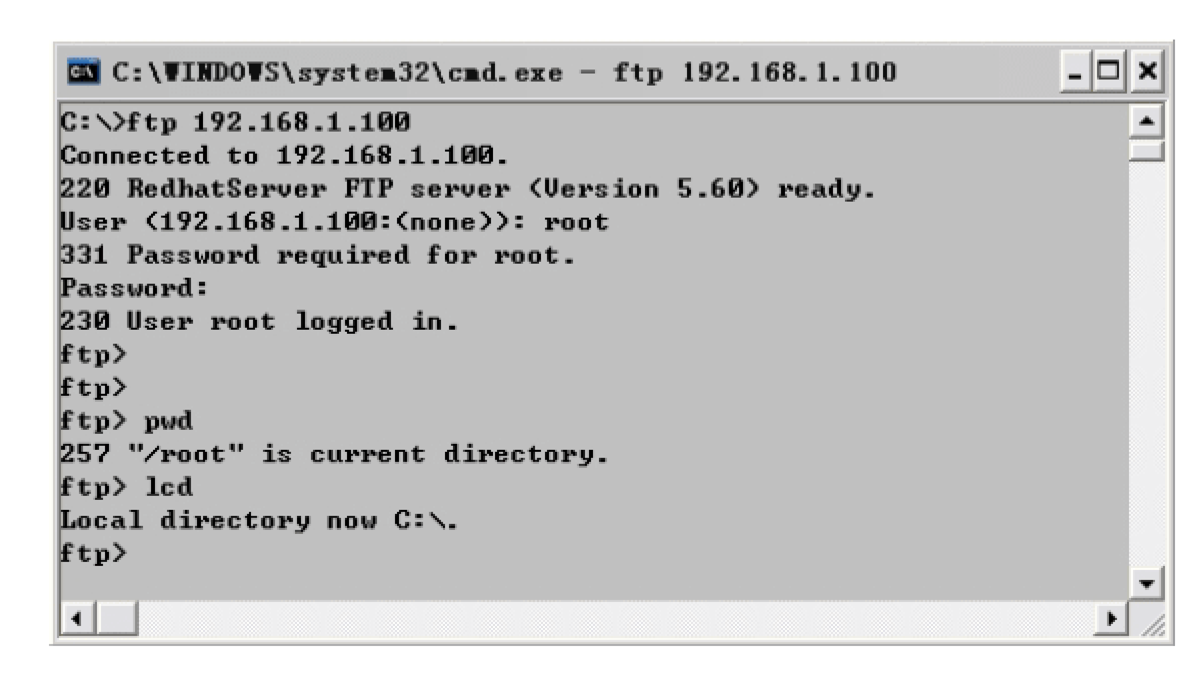

```
C:\>ftp 192.168.1.100
Connected to 192.168.1.100.
220 RedhatServer FTP server (Version 5.60) ready.
User (192.168.1.100:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp>
ftp>
ftp> pwd
257 "/root" is current directory.
ftp> lcd
Local directory now C:\.
ftp>
```

图 3-20　FTP 命令-PWD LCD

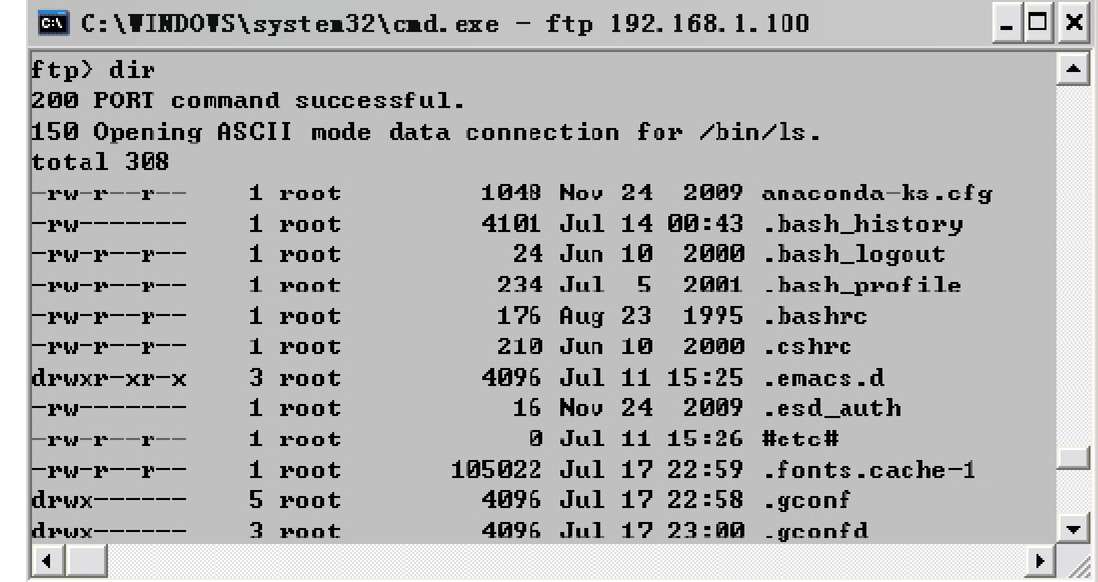


图 3-21　FTP 模式下的 Dir 命令

- ❑ Mget 命令：从远程服务器上下载多个文件，使用空格分隔文件名，或使用通配符下载批量文件，语法格式为 Mget [文件名列表]或使用通配符。例如，从远程 Linux 主机中/etc/log 目录下载所有 Log 文件，可使用命令 Mget *.log。

注意：（1）Get 命令将从 Linux 系统当前目录下载文件到客户端主机当前目录，使用 Lcd 命令，可查看客户端主机的当前目录。

（2）如需查看 Get 命令下载进度，可先执行 hash 命令，即可看到#符号的下载进度。

Get 命令执行结果如图 3-22 所示。

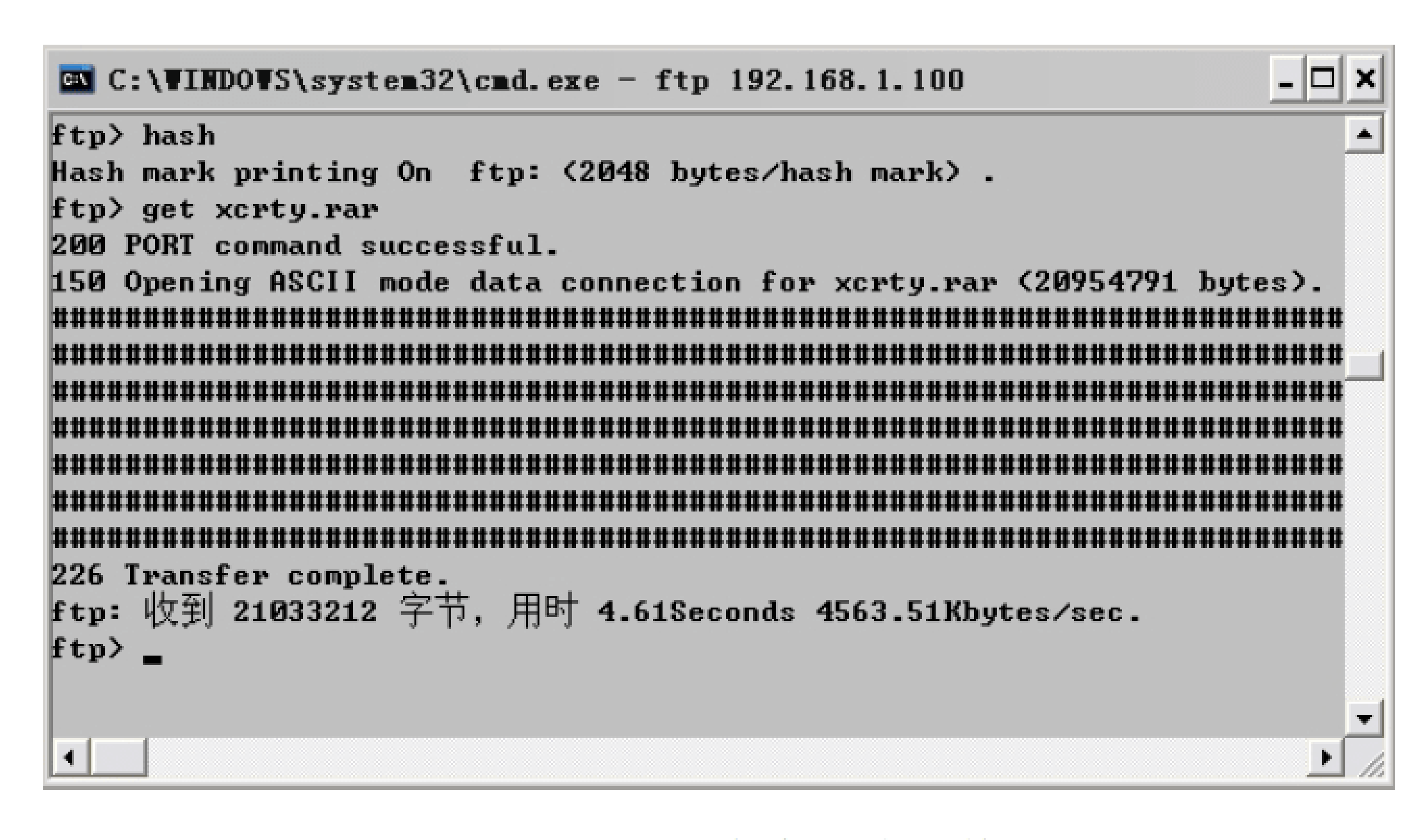

```
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> get xcrty.rar
200 PORT command successful.
150 Opening ASCII mode data connection for xcrty.rar (20954791 bytes).
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
226 Transfer complete.
ftp: 收到 21033212 字节，用时 4.61Seconds 4563.51Kbytes/sec.
ftp>
```

图 3-22　Get 命令下载文件

4．Put 与 Mput 命令

- ❑ Put 命令：从客户端上传文件至远程服务器，语法为 Put　[文件名]。
- ❑ Mput 命令：上传批量文件，语法为 Put [文件名列表]或使用通配符。使用 Mput 命令上传多个文件时，每上传完一个文件都会询问是否上传下一个文件，在确认后即开始上传，如图 3-23 所示。

由于 FTP 服务器的主要功能是用于上传和下载文件，所以上面介绍了与上传和下载相关的命令，其他应用命令可以查阅相关 FTP 资料。



图 3-23　Mput 命令上传多个文件

3.2.4　Telnet 协议

Telnet（远程登录协议）协议是 TCP/IP 协议族中的一种。用户可通过该协议远程访问服务器、网络设备（如交换机和路由器、防火墙）等，并通过命令行的方式实现远程控制。而且，一旦远程登录成功后，即拥有了完全控制远程设备的权限。该协议极大地简化了网络维护的烦琐，是网络管理人员最常用的协议之一，该协议使用 TCP 23 端口。

Telnet 协议的最大特点是能够实现异构设备、异构系统之间的互访。例如，通过计算机能够连接路由器设备，通过 Windows 系统能够登录交换机操作系统。在连接过程中，Telnet 协议使用 ASCII 字符集转换为控制命令实现交互。

电子公告牌（BBS）是一种典型的 Telnet 协议应用，登录用户均通过 Telnet 协议实现连接，并完成书写和发布消息等操作。下面具体介绍 Telnet 协议的应用。

3.2.4.1　开启 Telnet 登录允许

要使用 Telnet 协议远程登录设备，首先需开启远端设备的 Telnet 服务支持，即允许 Telnet 方式登录。在第 2 章节的交换机部分已经介绍了如何开启 H3C 和 Cisco 交换机 Telnet 服务。下面分别介绍在 Windows 系统、Linux 系统上开启 Telnet 服务。

1．Windows 系统开启 Telnet

此处以 Windows Server 2003 为示例。选择【控制面板】|【服务】选项，并选择列表中的 Telnet 服务，可看到该服务的运行状态。将其状态设置为启动后，该主机允许其他设备远程 Telnet 登录，如图 3-24 所示。



图 3-24　Windows 系统中 Telnet 服务的运行状态

2．Redhat Linux 系统开启 Telnet

在 Redhat Linux 系统中，首先通过命令查看是否已经安装了 Telnet 程序。如果能够查

找到程序，则表示已经安装。在 Linux 系统命令行模式下，使用如下命令：

```
[root@RedhatServerroot]#rpm -q telnet
telnet-0.17-25
```

通常，RedHat Linux 默认会安装该服务，但如果没有查询到安装包，那么还需要从 Linux 安装光盘中获取 telnet-server-0.17- 25.i386.rpm 的安装包，并使用如下命令进行安装：

```
[root@RedhatServerroot]#rpm -i telnet-server-0.17-25.i386.rpm
```

确认安装 Telnet 程序后，还需要开启该服务，编辑/etc/xinetd.d/telnet 文件，命令如下：

```
[root@RedhatServerroot]#vi /etc/xinetd.d/telnet
```

在该文件中，找到代码行 disable = yes，并将参数 yes 改成 no，如图 3-25 所示。

保存后退出，即开启了 Telnet 服务。接着使用命令将 Telnet 服务激活，执行如下命令：

```
[root@RedhatServerroot]#service xinetd restart
```

最后还需设置允许 root 账号通过 Telnet 远程登录，编辑文件/etc/pam.d/login，命令为：

```
[root@RedhatServerroot]#vi etc/pam.d/login
```

在该文件中，在代码行 auth required /lib/security/pam_security.so 前添加#，将该行注释掉，此时能够在 Windows 客户端中通过命令提示符界面远程登录 Linux 系统，如图 3-26 所示。


```
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = no
}
```

图 3-25　开启 Linux 系统 Telnet 服务

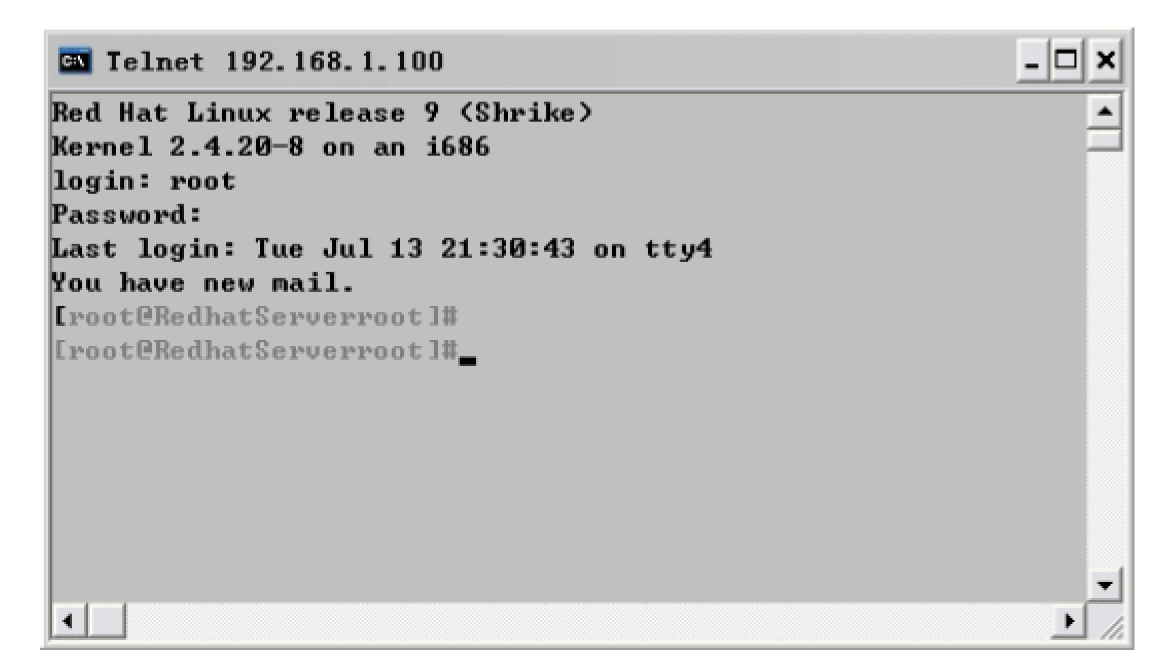


图 3-26　将命令提示符界面 Telnet 到 Linux 系统中

3.2.4.2　Telnet 工具和操作命令

Telnet 协议在网络维护中应用广泛。例如，可以 Telnet 方式登录 Windows、Linux 服务器，通过命令查看设备运行状态、上传下载文件等；可以 Telnet 方式登录到路由器、交换机或防火墙等网络设备，对其进行管理和配置。以下对常用的 Telnet 工具和命令应用进行介绍，内容如图 3-27 所示。



图 3-27　Telnet 命令的具体应用介绍

1．Windows 系统的 Telnet 程序

在 Windows 操作系统中自带了 Telnet 工具，可在命令提示符界面中使用该工具。其语法为：Telnet [远程服务器名称]或[IP 地址]。例如，远程登录交换机设备，如图 3-28 所示。

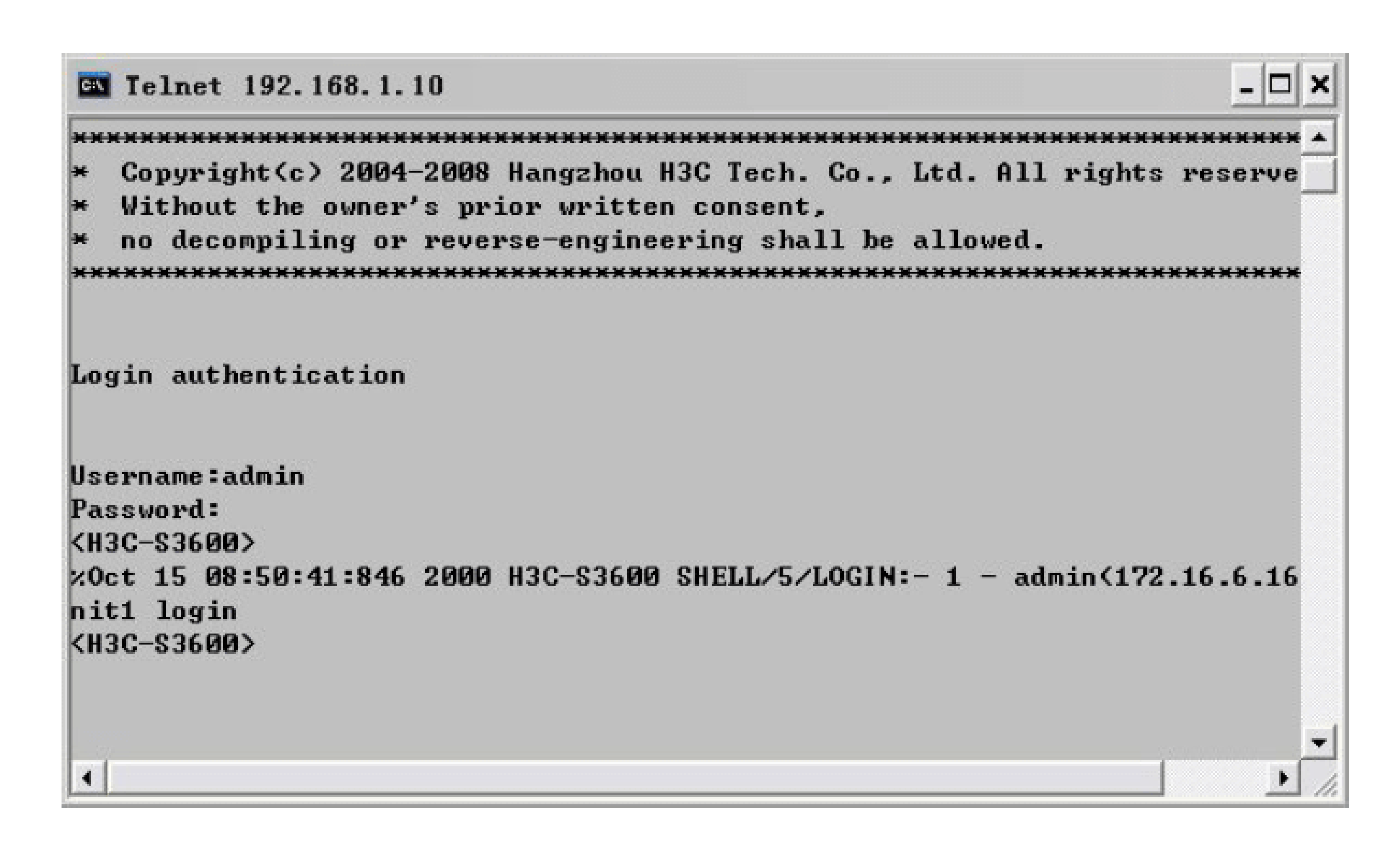


图 3-28　命令提示中使用 Telnet 命令

除 Windows 系统自带的 Telnet 程序外，还可下载第三方程序，如 SecureCRT。在程序界面中选择连接远程主机所采用的协议为 Telnet，输入目标 IP 地址后即可开始登录，如图 3-29 所示。

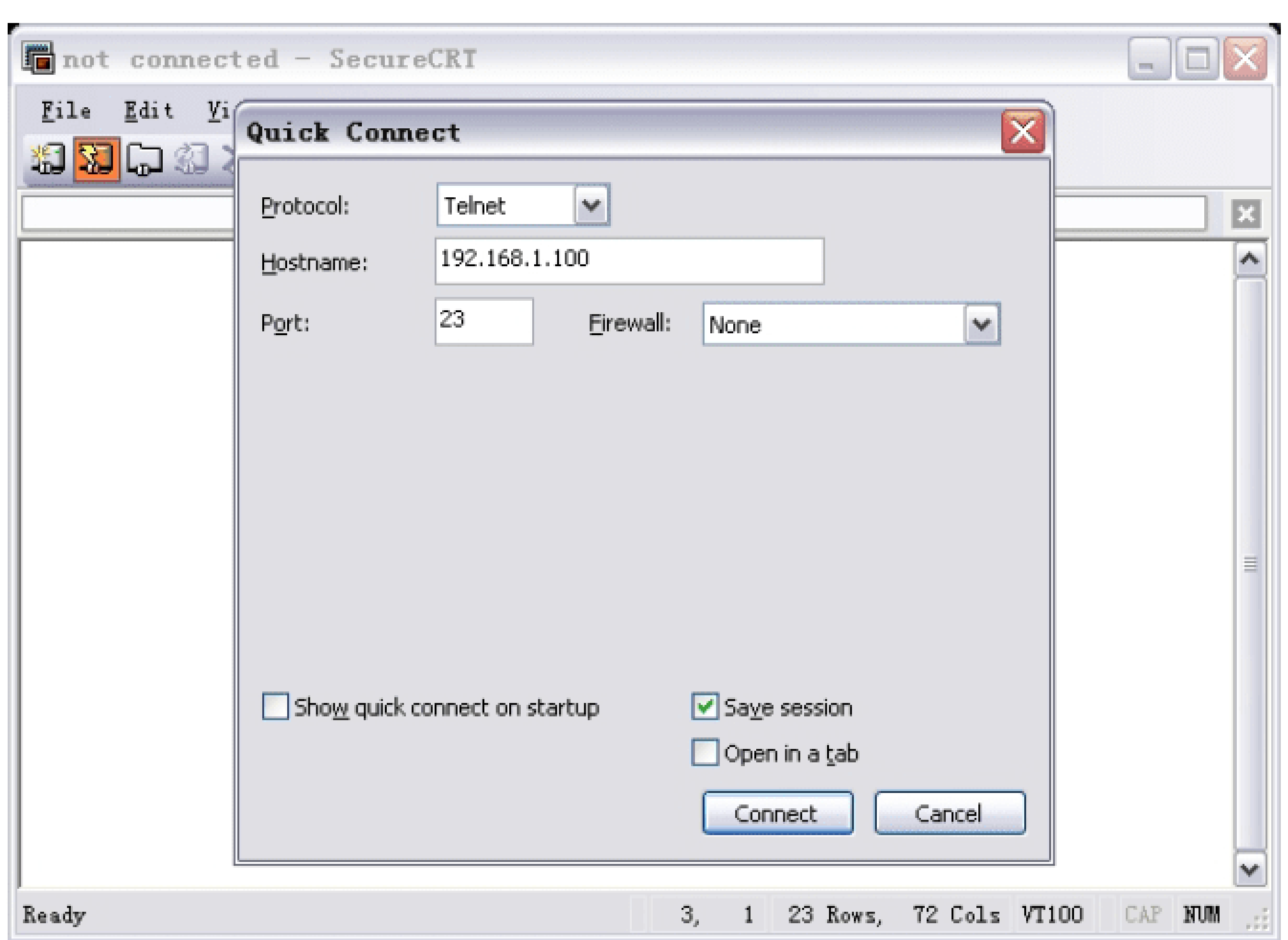


图 3-29　使用第三方的 Telnet 程序登录远程主机

2．Linux 系统的 Telnet 程序

在 Linux 操作系统中同样自带了 Telnet 程序，并可在图形界面和命令行界面中执行其命令。在 Redhat Linux 图形界面中，选择【主菜单】|【系统工具】|【终端】命令，打开命令执行窗口，即可使用 Telnet 命令。例如，连接远程到 Windows 服务器，输入用户名和密

码即可登录到服务器中，如图 3-30 所示。

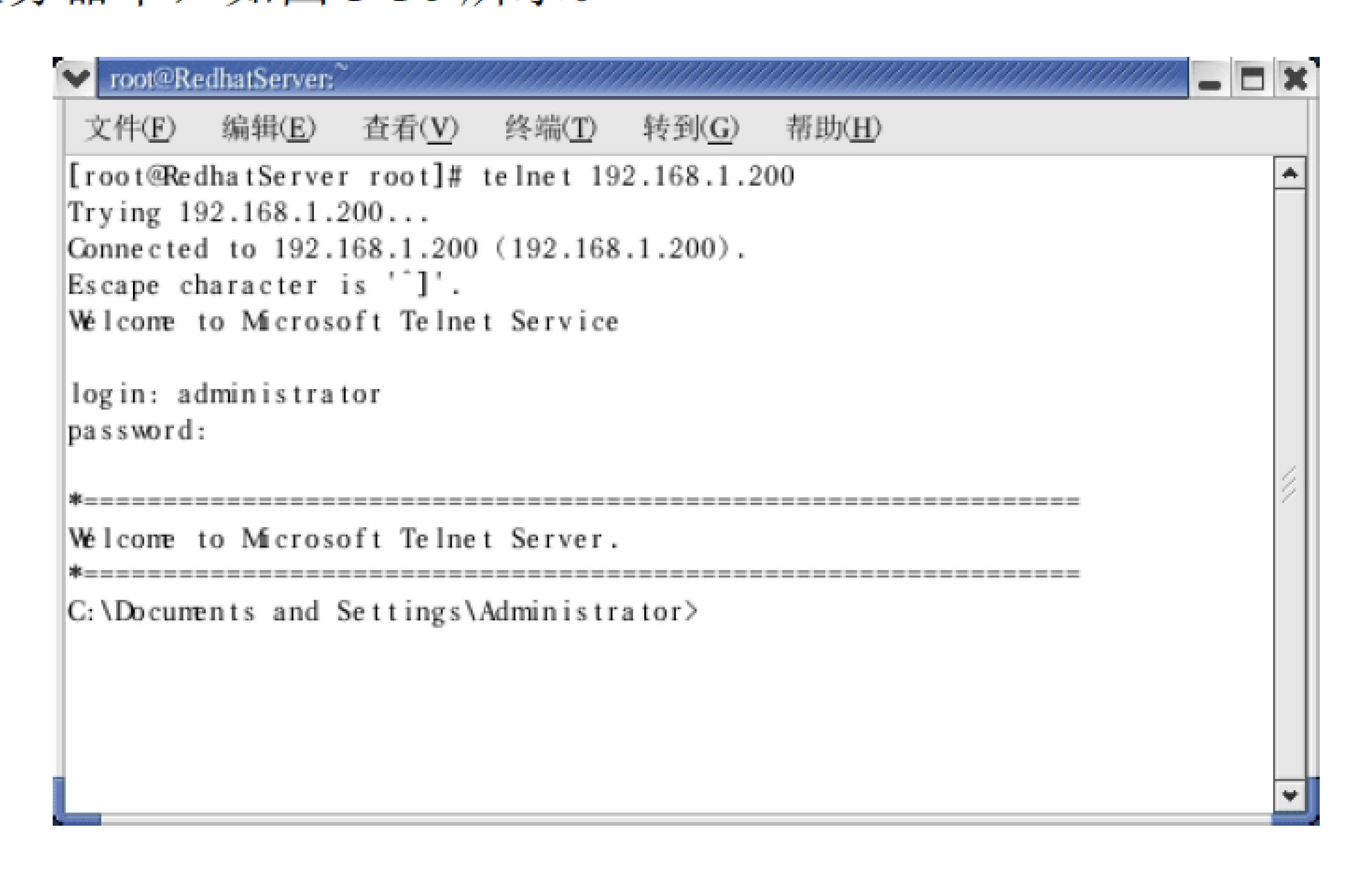


图 3-30　在 Linux 图形界面中使用 Telnet 命令

同样，在 Linux 命令行界面中，也可使用 Telnet 命令登录到远程 Windows 服务器中，如图 3-31 所示。

```
[root@RedhatServerroot]#telnet 192.168.1.200
Trying 192.168.1.200...
Connected to 192.168.1.200 (192.168.1.200).
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login:
login: administrator
password:

*===============================================================
Welcome to Microsoft Telnet Server.
*===============================================================
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
```

图 3-31　在 Linux 命令行界面中使用 Telnet 命令

3.2.4.3　Telnet 登录服务器常用命令

使用 Telnet 命令能够获得与远程服务器用户相同的权限。那么，使用 Telnet 命令登录 Windows 服务器时，登录用户便拥有了 DOS 命令操作许可，包括查看文件列表、复制和删除文件等，但其操作命令较少。

登录 Linux 系统时，Telnet 用户同样具备使用所有 Linux 命令的权限。Linux 系统对命令方式操作提供了完全的支持，包括文件管理、系统管理、网络维护等。换言之，使用命令能够完成所有 Linux 系统的工作。此处通过几个常用的 Linux 命令介绍在 Telnet 模式下登录 Linux 系统可实现的操作。

（1）Ifconfig 命令：查看 Linux 系统网络配置，该命令与 Windows 系统中的 Ipconfig 命令相似。Telnet 模式下执行该命令，如图 3-32 所示。

（2）查看资源利用率命令：Top（查看 CPU 利用率）、Df（查看磁盘利用率）、Free（查看内存利用率）。其中，Df 和 Free 命令执行结果如图 3-33 所示。

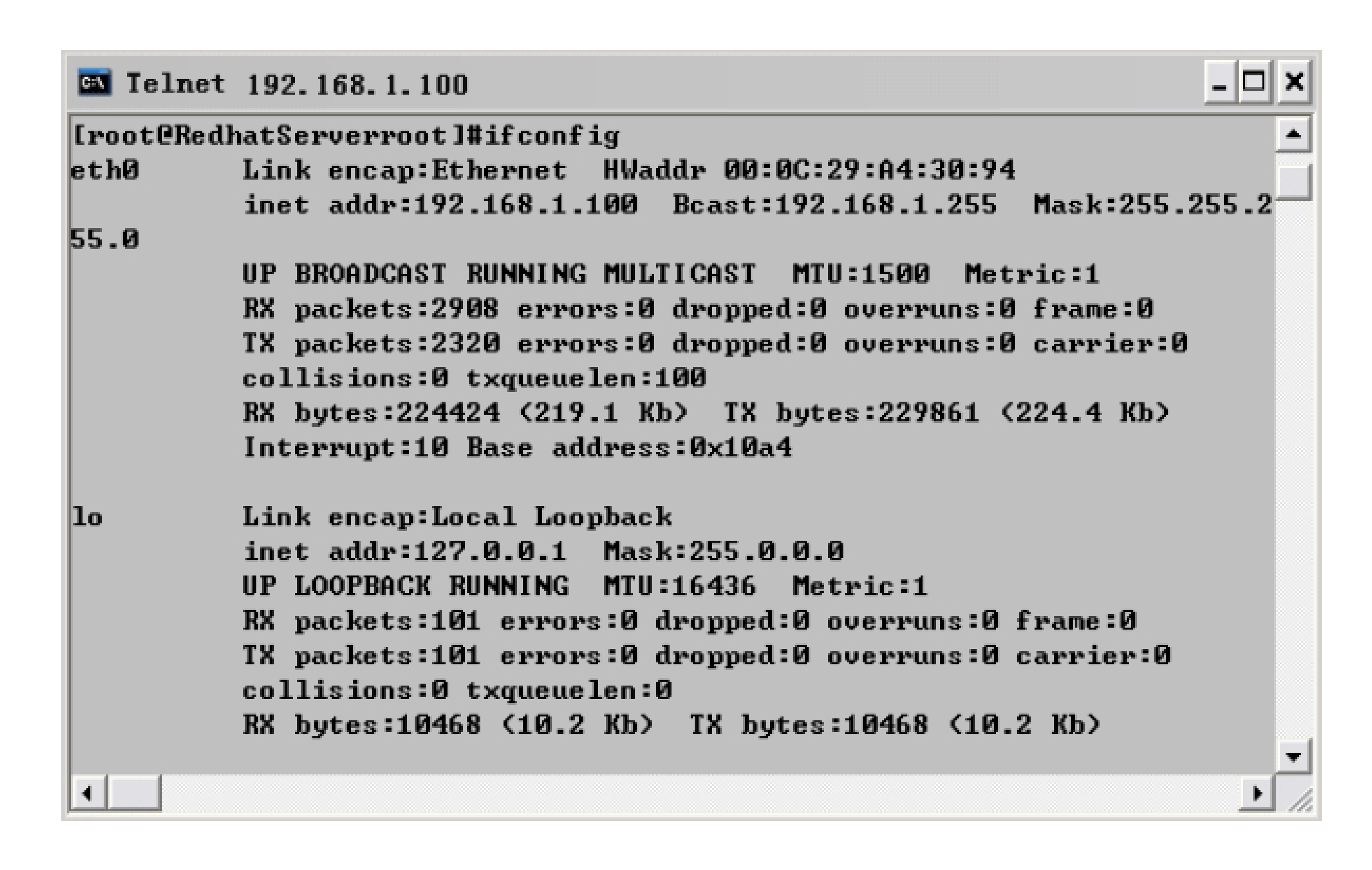


图 3-32　Telnet 模式下查看 Linux 系统网络配置

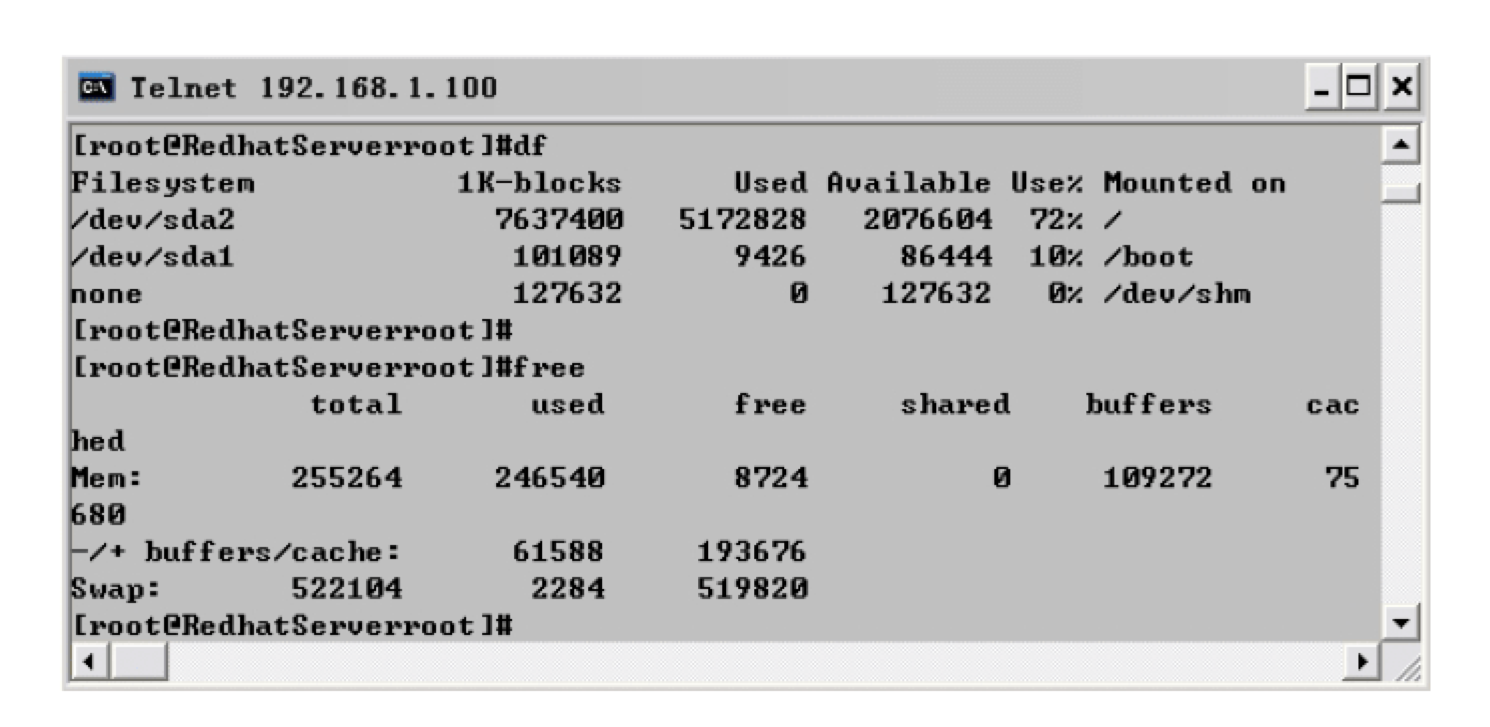


图 3-33　Telnet 模式下查看 Linux 系统资源利用率

（3）RM 和 Rmdir 命令：删除文件及文件夹。需要注意的是，使用 Rmdir 命令只能删除空文件夹，如果需要同时删除文件夹及其内容，可使用 Rm –r　[文件夹]命令，这 3 个命令执行结果如图 3-34 所示。

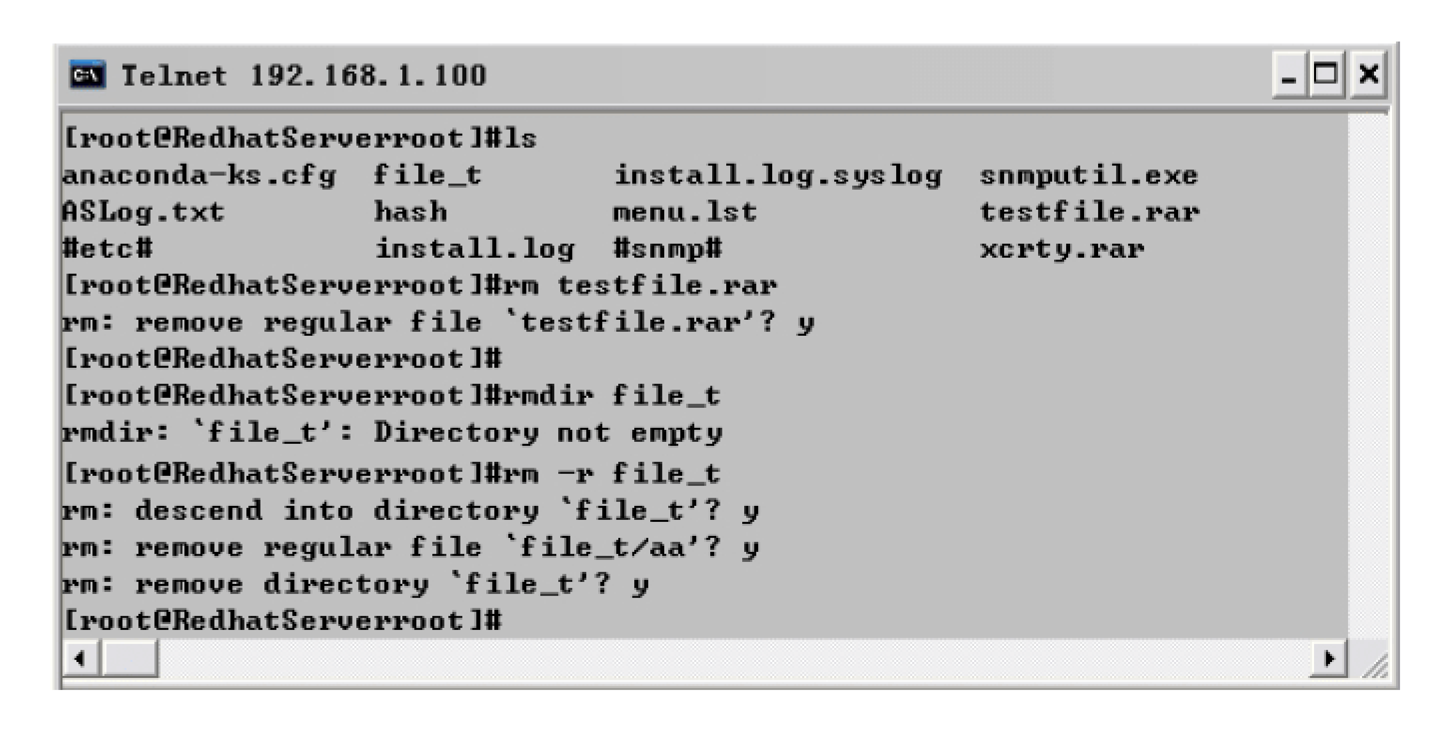


图 3-34　Telnet 模式下删除文件命令

3.2.4.4　Telnet 登录服务器实现上传和下载

Telnet 命令用于实现对远程服务器的控制，并不支持上传和下载文件。但如果需要在 Telnet 模式实现上传和下载，简单的方式是可通过 SecureCRT 工具 Telnet 登录到远程主机，然后使用 Sz 命令下载文件，使用 Rz 命令上传文件。使用 Sz 命令时需添加下载的文件

名，而使用 Rz 命令时，将会弹出对话框添加要上传的文件。两个命令执行结果如图 3-35 所示。

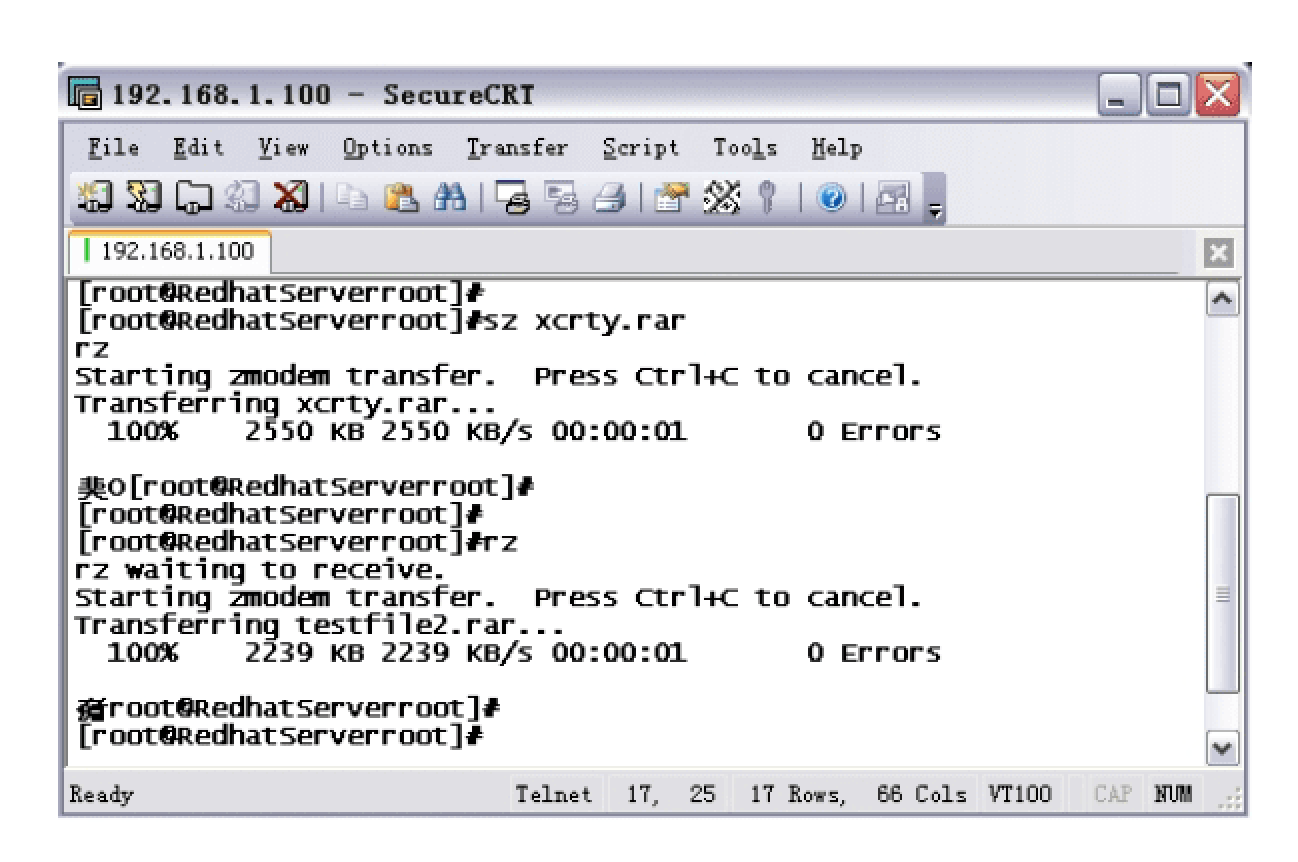


图 3-35 使用 SecureCRT 实现 Telnet 模式下的上传和下载

注意：Telnet 模式登录后，具有与服务器端主机用户同样的操作权限，可更改文件内容，也就是控制服务器端；而 FTP 模式操作权限较低，不能修改文件内容，只能够传输文件。

3.2.4.5 Telnet 登录网络设备的常用命令

Telnet 登录交换机、路由器等网络设备时，只需在网络设备侧开启允许 Telnet 登录，以及获取登录的口令，就可以登录网络设备进行完全控制。交换机开启 Telnet 及常用配置命令在本书第 2 章交换机设备部分进行了介绍，此处仅演示登录后的界面，如图 3-36 所示。

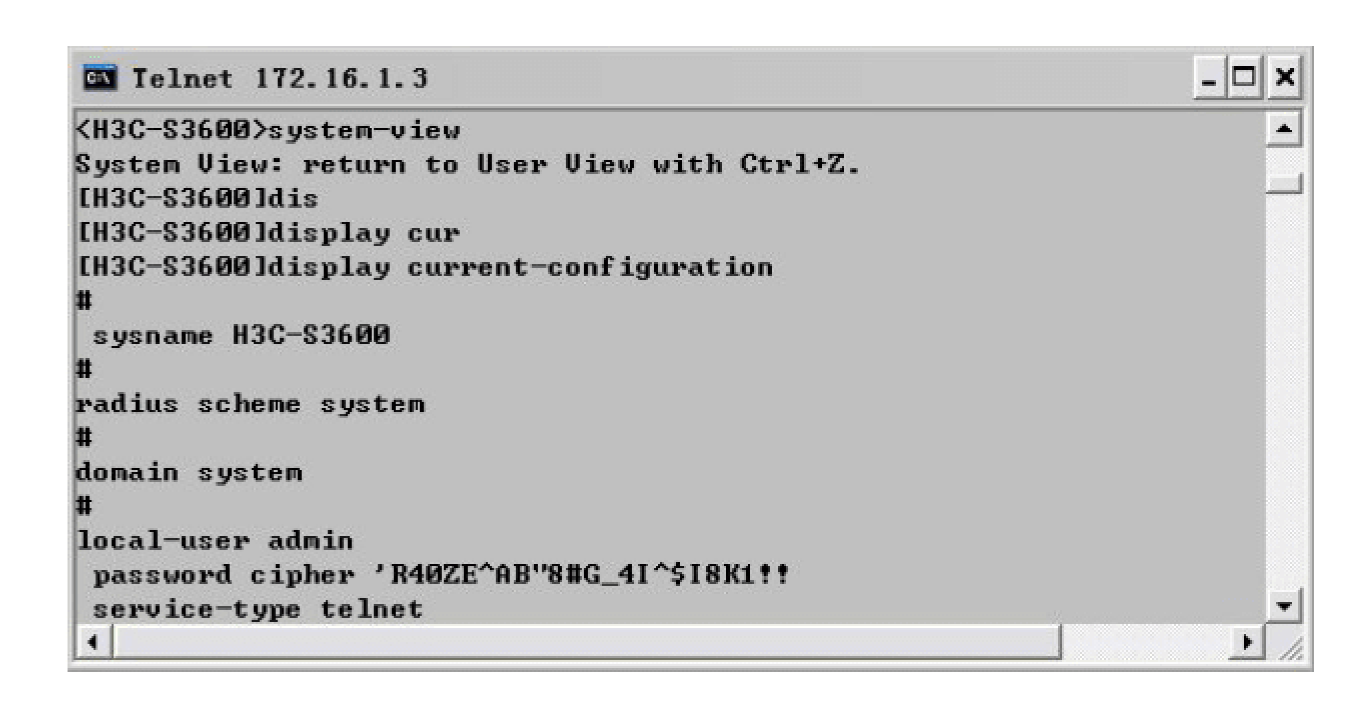


图 3-36 使用 Telnet 登录交换机设备

注意：在使用 Telnet 命令登录某网络设备后，还可通过该设备 Telnet 到另外一台设备上。

3.2.4.6 Telnet 应用——远程桌面连接

远程桌面连接同样使用的是 Telnet 协议，它是 Telnet 协议的扩展应用。远程桌面连接，就是客户端通过该方式连接到远程服务器时，将在客户端窗口界面中以图形界面实时操作远程服务器，包括安装、卸载和运行程序等。

Windows Server 2000/2003/2008 及 Windows XP 操作系统，都支持 Windows 客户端远

程桌面连接。Linux 系统同样支持 Windows 客户端通过远程桌面连接，但还需在客户端安装第三方支持的软件。以下介绍在 Windows 客户端系统中，通过远程桌面分别连接 Windows 系统和 Linux 系统，如图 3-37 所示。

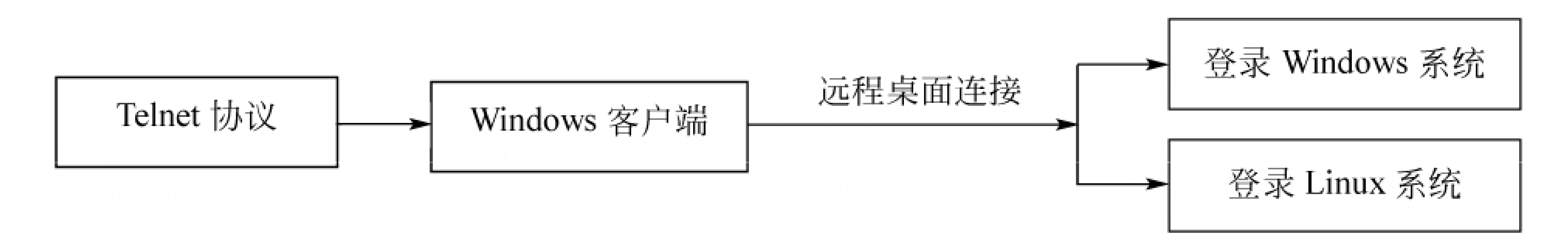


图 3-37　Windows 作为客户端远程桌面连接

1. Windows XP 客户端远程桌面连接 Windows Server 2003 系统

使用远程桌面连接目标主机，必须满足以下两个条件：

- ❑ 远程 Windows 服务器端中已经安装了支持桌面连接的服务组件。
- ❑ 远程 Windows 服务器端允许通过远程桌面方式登录。

首先在远程服务器安装远程连接组件，此处以 Windows Server 2003 操作系统为例。在 Server 版本中，该服务被称为“终端服务器”。选择【控制面板】|【添加或删除程序】|【添加\删除 Windows 组件】选项，并选择【终端服务器】复选框，即可开始组件安装，如图 3-38 所示。

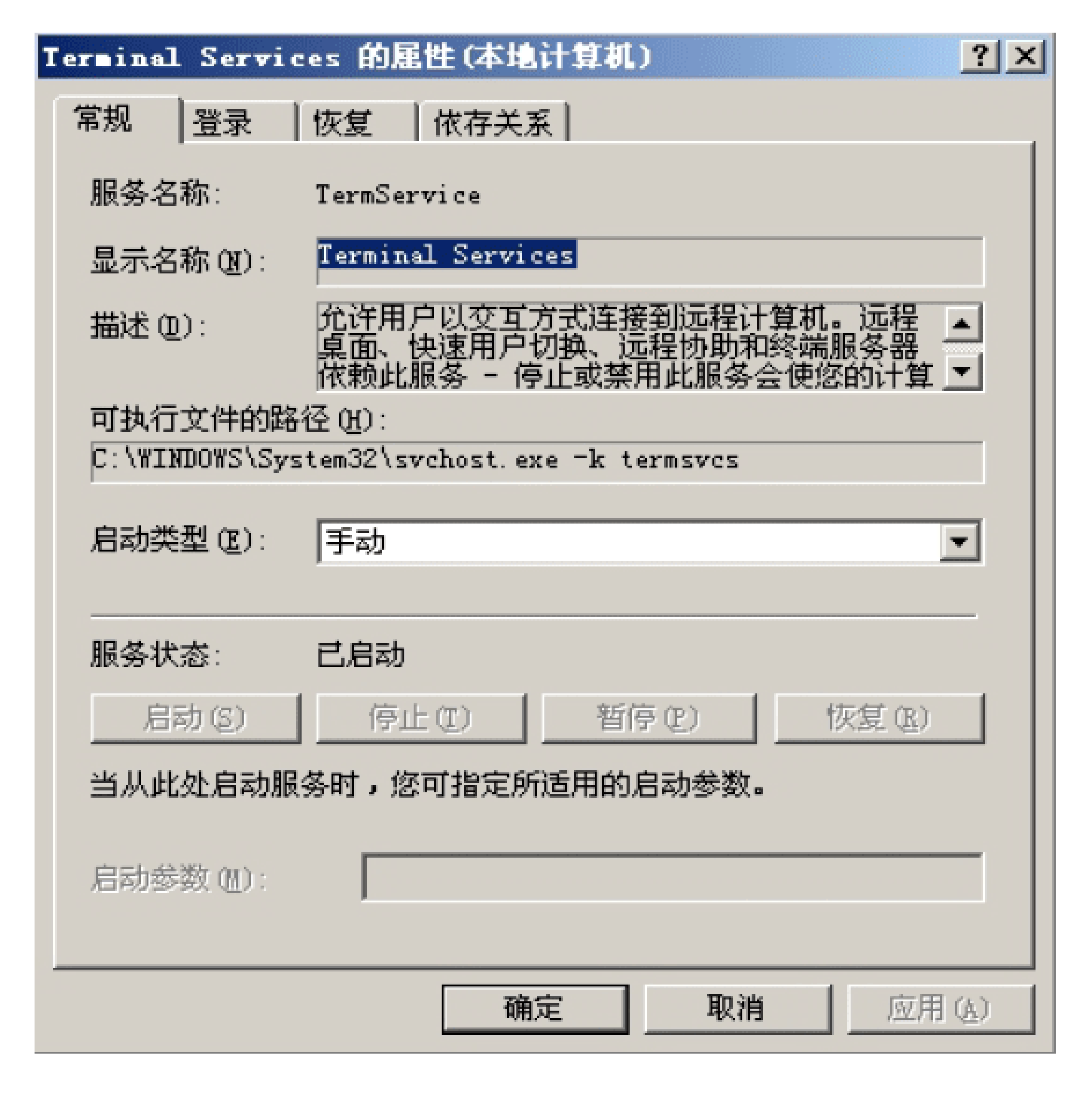


图 3-38　Windows Server 2003 中安装终端服务组件

安装组件完成之后，选择【控制面板】|【服务】|【Terminal Services】选项，可看到该服务已经正常运行，如图 3-39 所示。

最后需要设置允许远程登录该 Windows Server 2003 主机，在【我的电脑】上打开右键菜单并选择【属性】命令，然后在【远程】页面中选择【启用这台计算机上的远程桌面】复选框，即开启了远程登录的允许，如图 3-40 所示。

注意：如果远程 Windows 主机中安装了软件防火墙，则需开启防火墙允许远程登录。



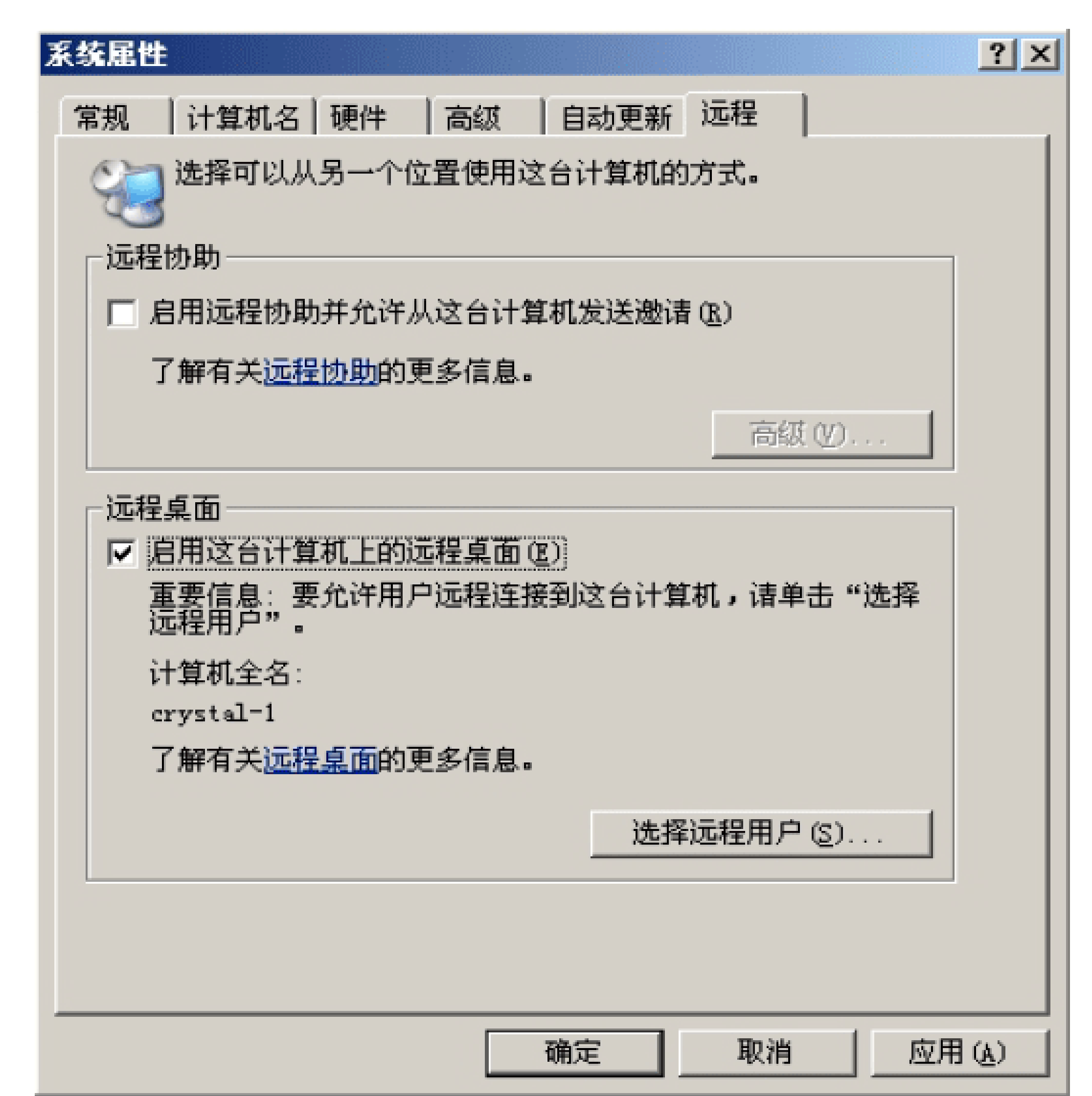


图 3-39　查看终端服务是否启动　　图 3-40　Windows Server 2003 系统中允许远程桌面连接

远程服务器主机设置完成后，即可在客户端主机中选择开始菜单中的【程序】|【附件】|【远程桌面连接】命令。或者在开始菜单的【运行】中输入 mstsc 命令打开连接窗口，输入目的 IP 地址后即可开始登录，如图 3-41 所示。

在连接远程主机后输入登录口令，即可完全控制远程主机，如图 3-42 所示。



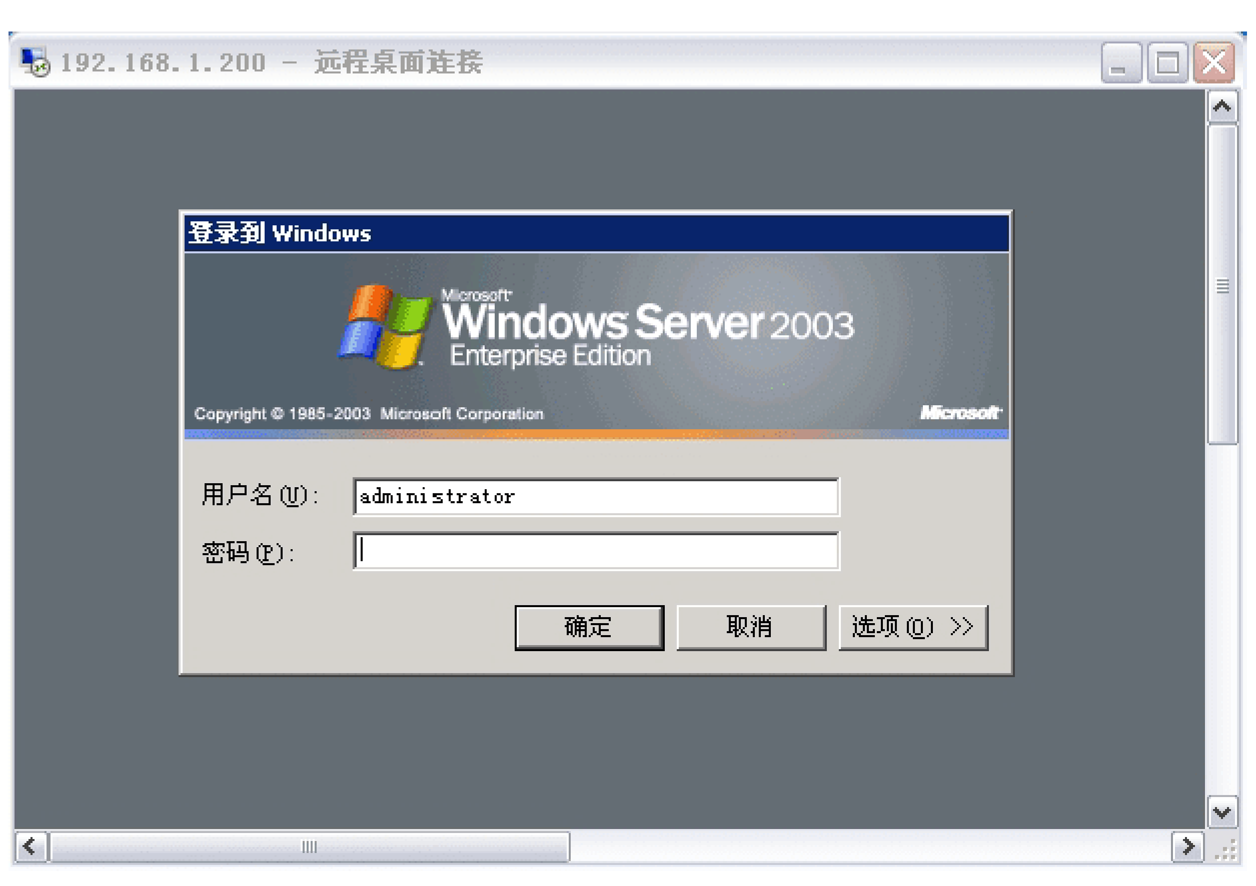


图 3-41　使用远程桌面连接登录远程服务器　　图 3-42　远程桌面连接登录服务器

如果要在远程主机与本地主机间实现文件的复制，则需要将本地的磁盘完全共享到远程服务器中。在【远程桌面连接】窗口中，选择左下角的【选项】，然后在【本地资源】页面单击【详细信息】按钮，在弹出界面中选择需共享的磁盘即可，如图 3-43 所示。

设置完成后，再次登录到远程主机中，打开我的电脑，将看到客户端共享的磁盘映射。此时，可将远程主机文件复制到映射磁盘中，或者将映射磁盘中的文件复制到远程主机中，以实现文件的传递，如图 3-44 所示。

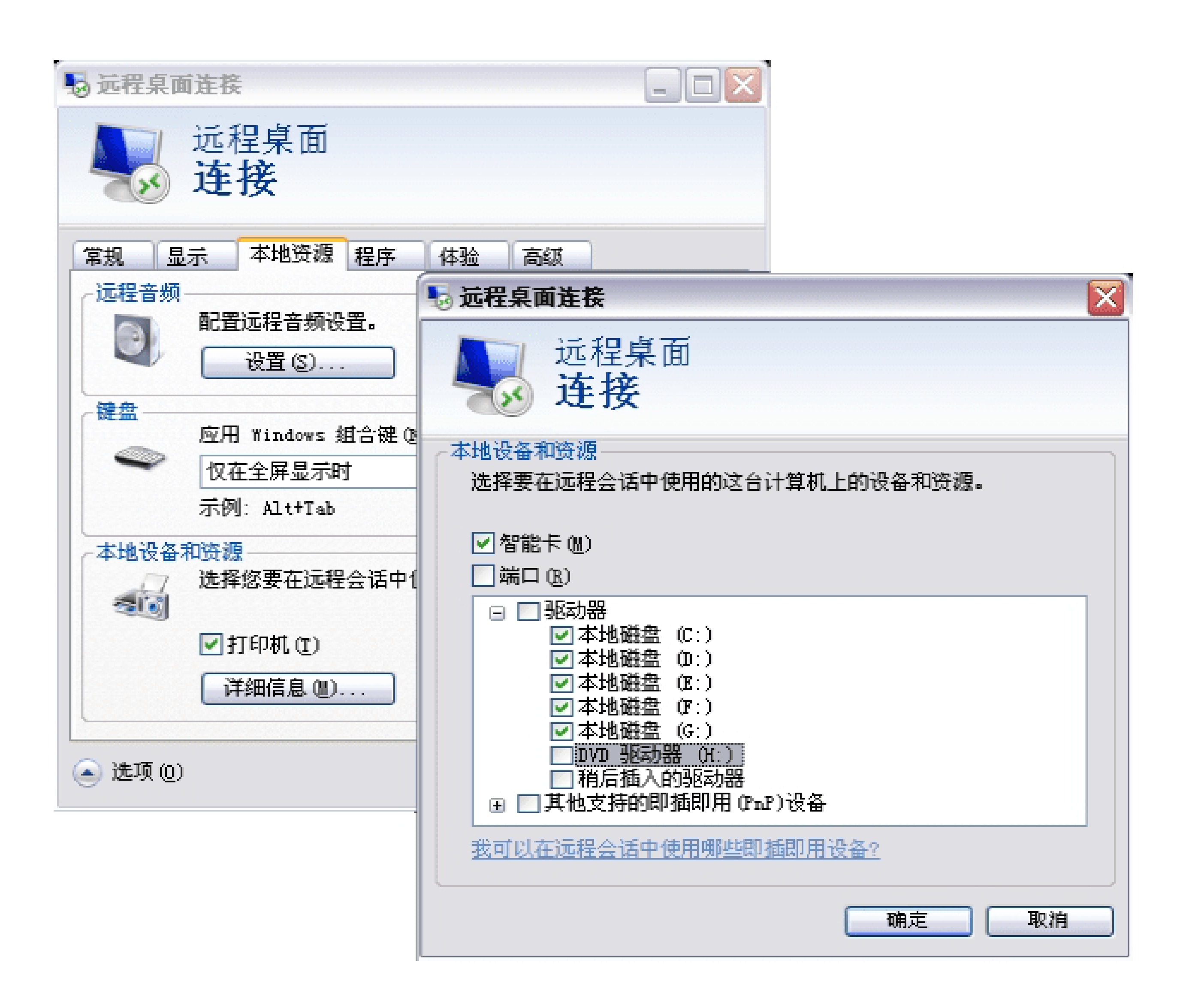


图 3-43　远程桌面连接附加设置——磁盘共享

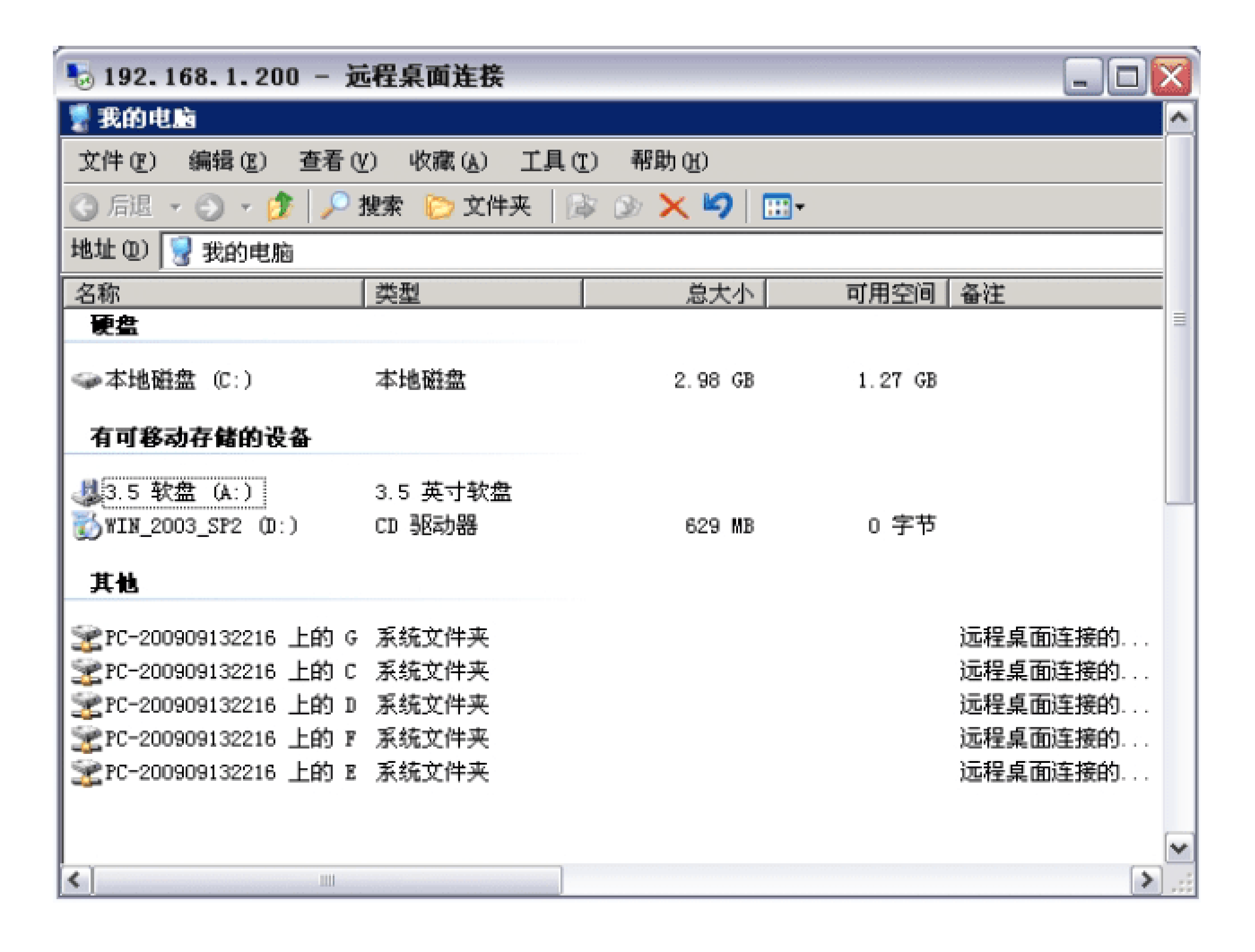


图 3-44　远程主机中通过映射磁盘完成文件的传递

2. Windows XP 客户端远程桌面连接 Linux 系统

Windows 系统中，可方便地使用远程桌面连接实现互访。但是该程序并不能与 Linux 系统兼容，所以需要下载和安装名为 XServer 的软件，以实现 Windows 系统下图形化显示 Linux 系统。同时，还需要下载支持 SSH/Telnet 协议的程序，以实现对 Linux 系统界面的转发。

此处推荐使用免费的 XServer 程序 Xming，以及免费的远程登录程序 PuTTy，以实现 Windows 系统下的远程桌面连接 Linux。具体的实现过程如下。

（1）配置 Linux 系统允许 X 桌面的转发。编辑文件/etc/ssh/sshd_config，执行如下命令：

```
[root@RedhatServerroot]#vi /etc/ssh/sshd_config
```

在文件中，将代码行 X11Forwrding yes 前的注释符号#去掉即可。

（2）下载并安装 Xming 程序。启动程序后，不需要进行任何配置，在托盘区出现 X 图标，说明程序已经正常运行。需要注意的是，此时还需下载安装 Xming 的字体，安装包名为 Xming-fonts 7.4.0.3，在显示 Linux X 桌面内容时，需要用到这些字体。

（3）配置 PuTTY。开启 PuTTY 程序，在 Connection | SSH | X11 页面中，选择 Enable X11forwarding 选项，并在 X display location 文本框中输入显示的桌面代码，此处填写 localhost:0，如图 3-45 所示。

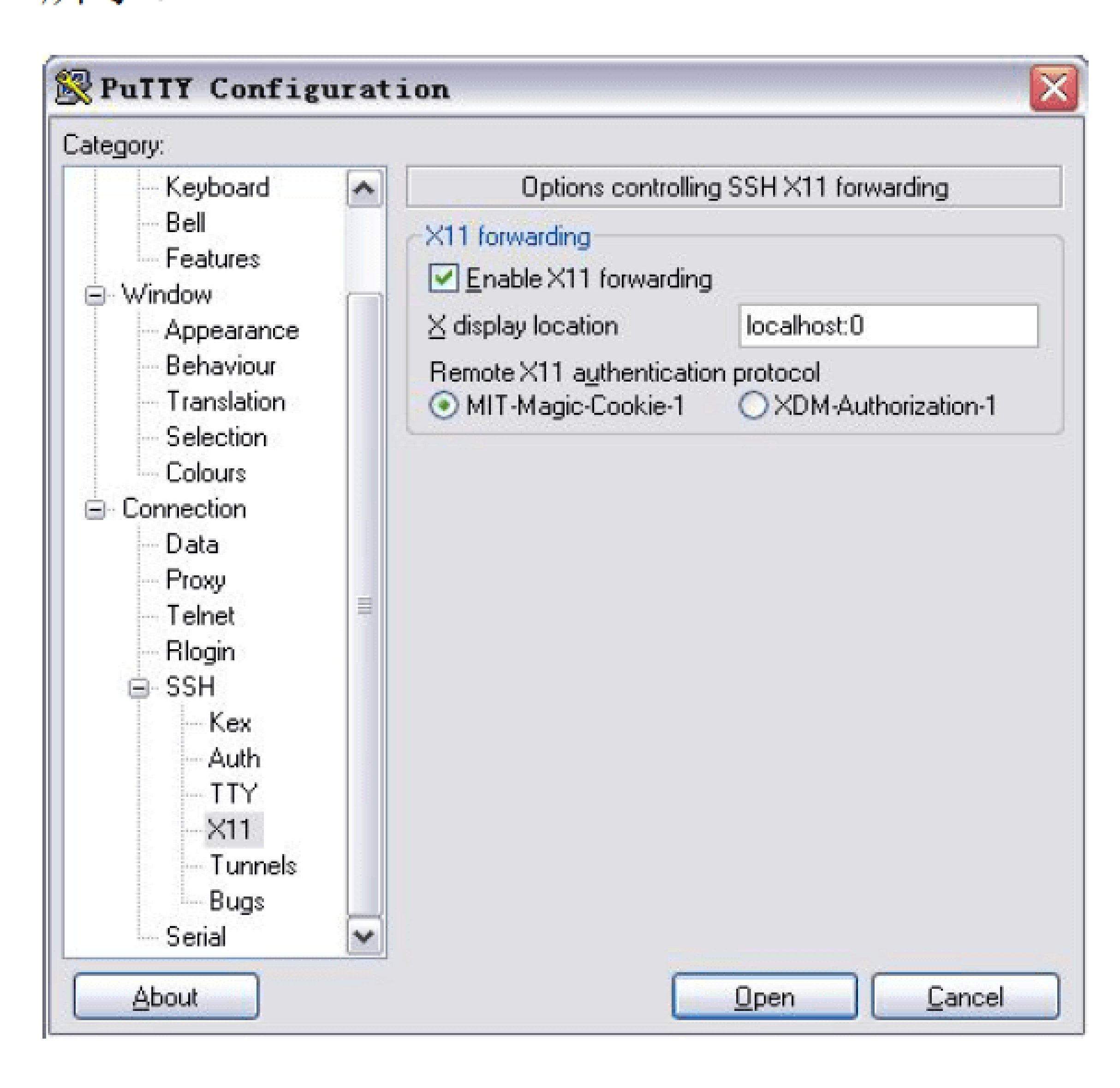


图 3-45　配置 PuTTY 开启对 X 界面的转发

（4）在 PuTTY 程序的 Session 页面中，输入对端 Linux 系统的 IP 地址（192.168.1.100），然后单击 Open 按钮，登录到对端 Linux 系统中，然后在登录的终端界面中输入转发命令 emacx &，如图 3-46 所示。



图 3-46　在 PuTTY 登录界面输入转发命令

输入该命令后将在 Windows 系统中弹出 Linux 图形化界面，如图 3-47 所示。

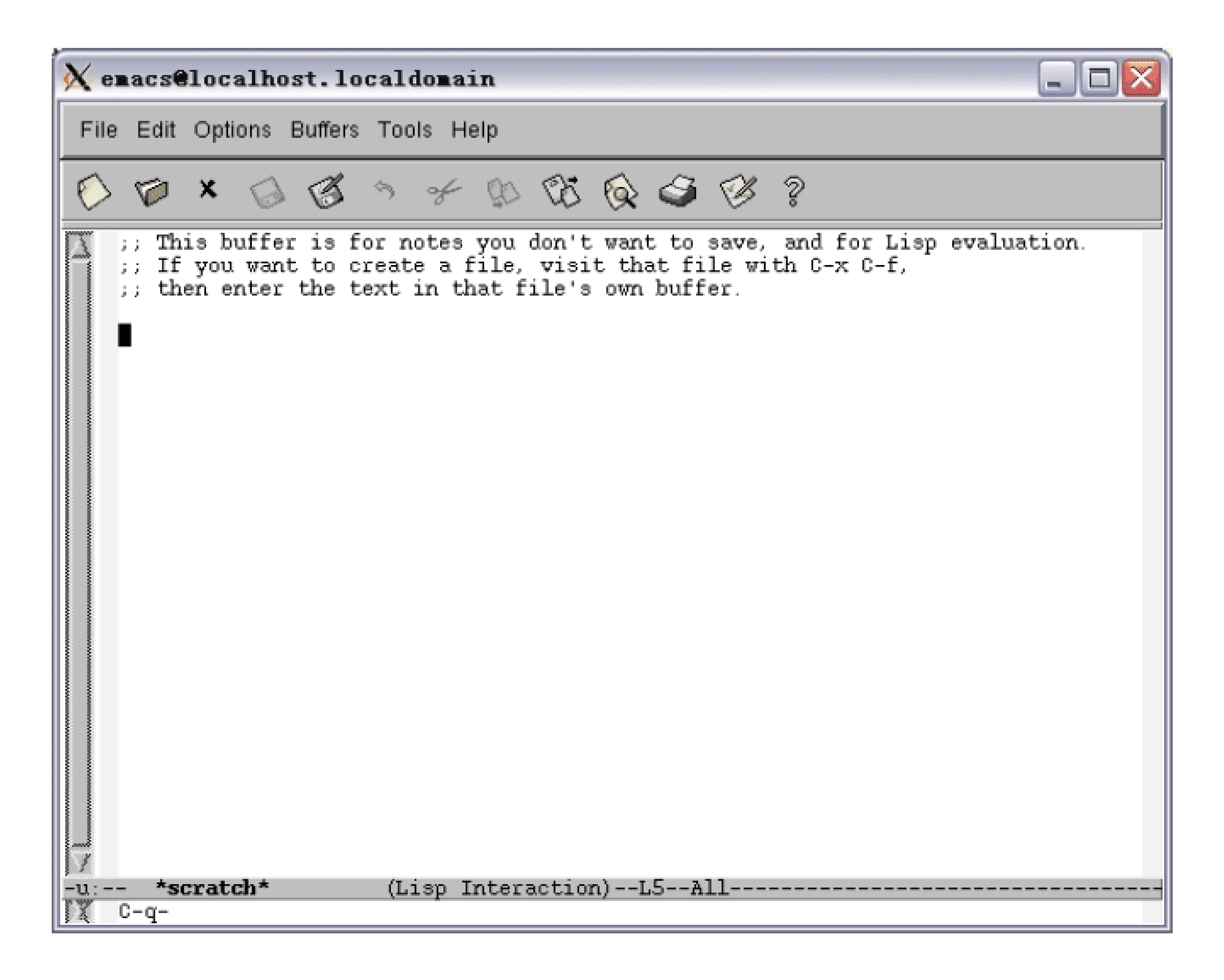


图 3-47　Windows 系统中显示远程 Linux 图形化界面

以上便完成了通过 Windows XP 客户端的远程桌面连接，实现了对 Windows Server 2003 系统和 Redhat Linux 系统的图形化访问。

3.2.5　SSH 协议

SSH（Secure Shell Protocol，安全外壳协议），该协议同样是一种远程连接协议。SSH 协议是 Telnet 和 FTP 协议的结合，即能够实现安全的远程连接，又能够实现文件复制、文件上传和下载的功能。该协议通过数据加密和压缩技术，以提高数据的安全性和传输速率。

在 Telnet、FTP 等明文传输模式下，网络易受到“中间人”的网络攻击。该攻击方式截获访问口令或数据，并冒充远程服务器接收客户端的数据，然后将假冒的数据传给真正的服务器。而在 SSH 协议的密文传输方式下，中间人攻击方式截获的数据也是经过加密的，所以很难实现攻击。使用 SSH 协议能够有效地保证数据传输的安全性。

注意：Telnet 协议和 SSH 协议最大的区别在于，Telnet 是明文传输，而 SSH 采用密文传输。

1．SSH 协议的发展和历史

SSH 协议最早于 1995 年由芬兰一家公司开发。但由于版权和费用的原因，SSH 协议使用越来越少，取而代之的是免费的 OpenSSH 协议。此处仍以 SSH 协议做介绍，该协议经过不断发展，最后形成了两个版本，SSH1 和 SSH2，SSH1 又分为 1.3 和 1.5 两个版本，其采用了 RSA（非对称加密算法）来生成密钥，以及采用 CRC（循环冗余校验码）来确保数据的完整性，但该方式存在一定的缺陷。

SSH2 采用更为先进的 DSA（数字签名）等算法来代替 RSA 算法，且使用了 HMAC（消息证实代码）算法替代 CRC 算法，弥补了 CRC 算法的缺陷。

2. Redhat Linux 开启 SSH 服务支持

要通过 SSH 方式访问 Linux 服务器进行配置、文件传输等操作，首先需要配置 Linux 服务器开启 SSH 服务。操作步骤如下。

（1）进入到 Redhat Linux 系统命令行模式，验证是否已经安装了 SSH 程序，命令为：

```
[root@RedhatServerroot]#rpm -q sshd
```

如果未安装该程序，则需要下载安装包 ssh-2.3.0.tar.gz 进行安装。

（2）在安装 SSH 服务后，进入/etc/ssh/目录，将看到 SSH 协议的配置文件，名称为 Sshd_config，一般不需要对该配置文件做任何配置。

（3）使用命令重启 SSH 服务，命令为 sshd restart 或 service sshd restart，如下：

```
[root@RedhatServerroot]#service sshd restart
```

如果要在 Linux 图形界面中配置 SSH 服务，则需选择【系统设置】|【服务器设置】|【服务】命令，在服务配置界面中选择 sshd 复选框，并单击【开始】按钮启动该服务，如图 3-48 所示。

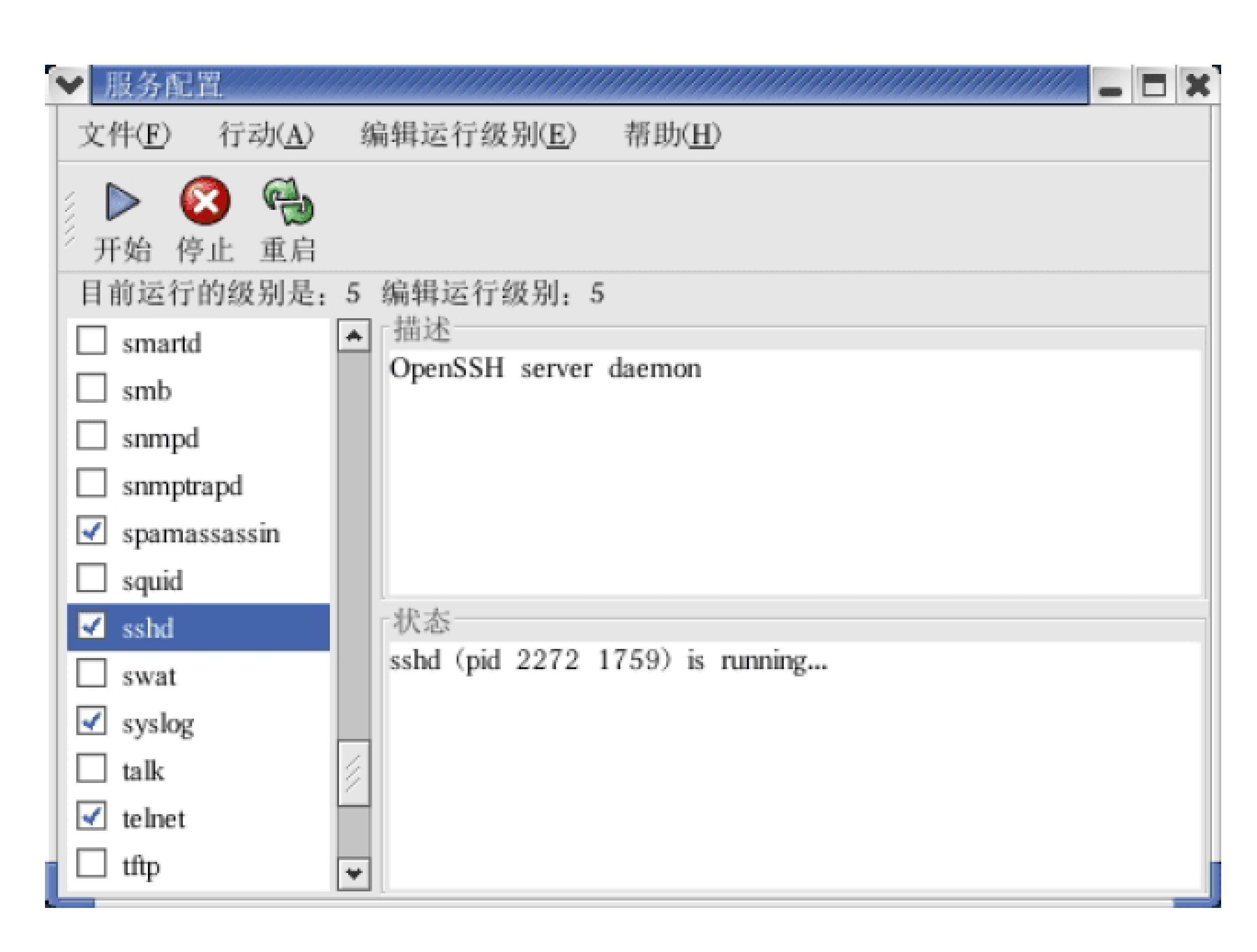


图 3-48 在 Linux 图形界面启动 SSH 服务

（4）此时，即可通过客户端软件 SecureCRT 以 SSH 模式远程登录 Linux 服务器。在程序主界面中，单击 Quick Connect 按钮，打开连接设置界面，选择协议为 SSH2，并输入 Linux 服务器 IP 地址后即可登录访问。连接和成功登录界面如图 3-49 所示。

3. Windows 服务器开启 SSH 服务支持

Telnet 和 SSH 方式登录远程 Windows 服务器，其命令方式操作仅限于 DOS 命令，实际操作意义并不大。所以在 Windows 操作系统中未提供 SSH 服务，但仍可以通过第三方的 SSH 程序实现 SSH 远程登录支持，此处推荐程序 F-Secure SSH。操作步骤如下：

（1）下载并安装 F-Secure SSH 的 Server 版本，并在远程 Windows Server 2003 系统中进行安装，如图 3-50 所示。

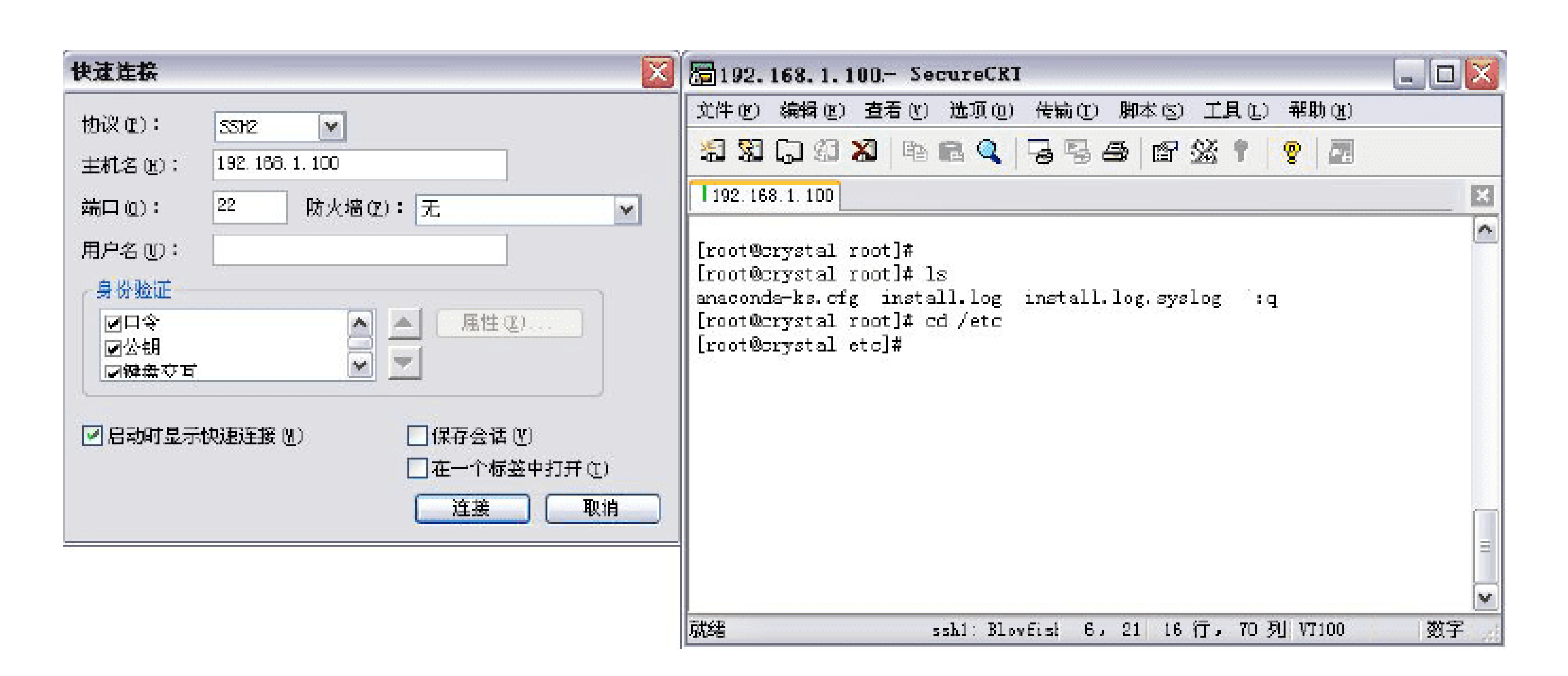


图 3-49　使用 SecureCRT 通过 SSH 模式连接远程 Linux 服务器

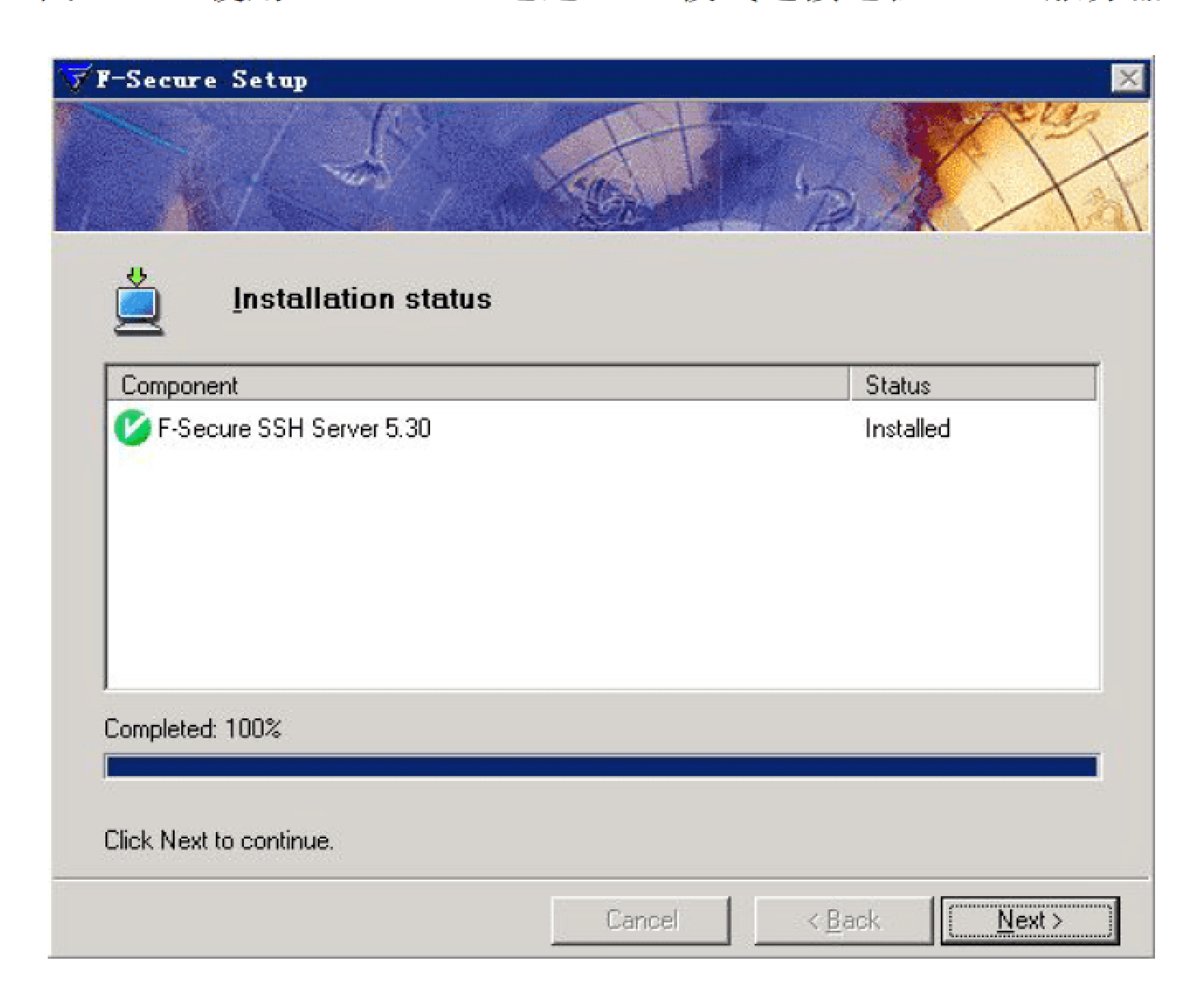


图 3-50　安装 F-Secure SSH Server 程序

（2）通常并不需要对 F-Secure SSH 程序进行配置，只需要确保该服务已经启动。选择 Windows 主菜单【程序】| F-Secure SSH Server | Configuration 项，打开该程序的配置界面，将看到其状态为启动状态，如图 3-51 所示。

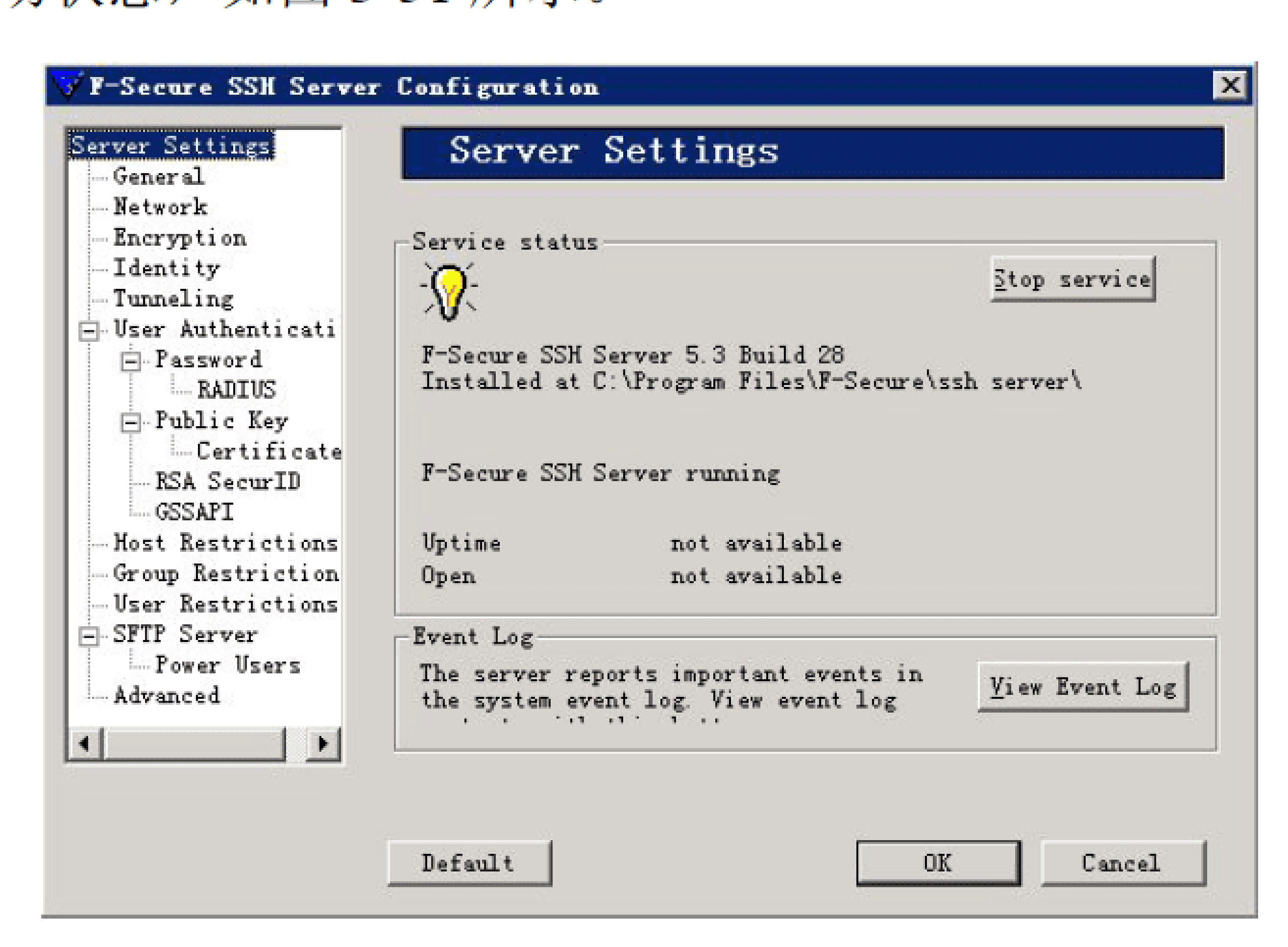


图 3-51　启动 F-Secure SSH 服务

（3）此时，在客户端主机中，可以通过 SSH 客户端工具进行远程访问，例如 SecureCRT 程序。选择登录协议为 SSH2，输入 IP 地址和登录口令后，即可远程以 SSH 方式登录 Windows 系统，如图 3-52 所示。

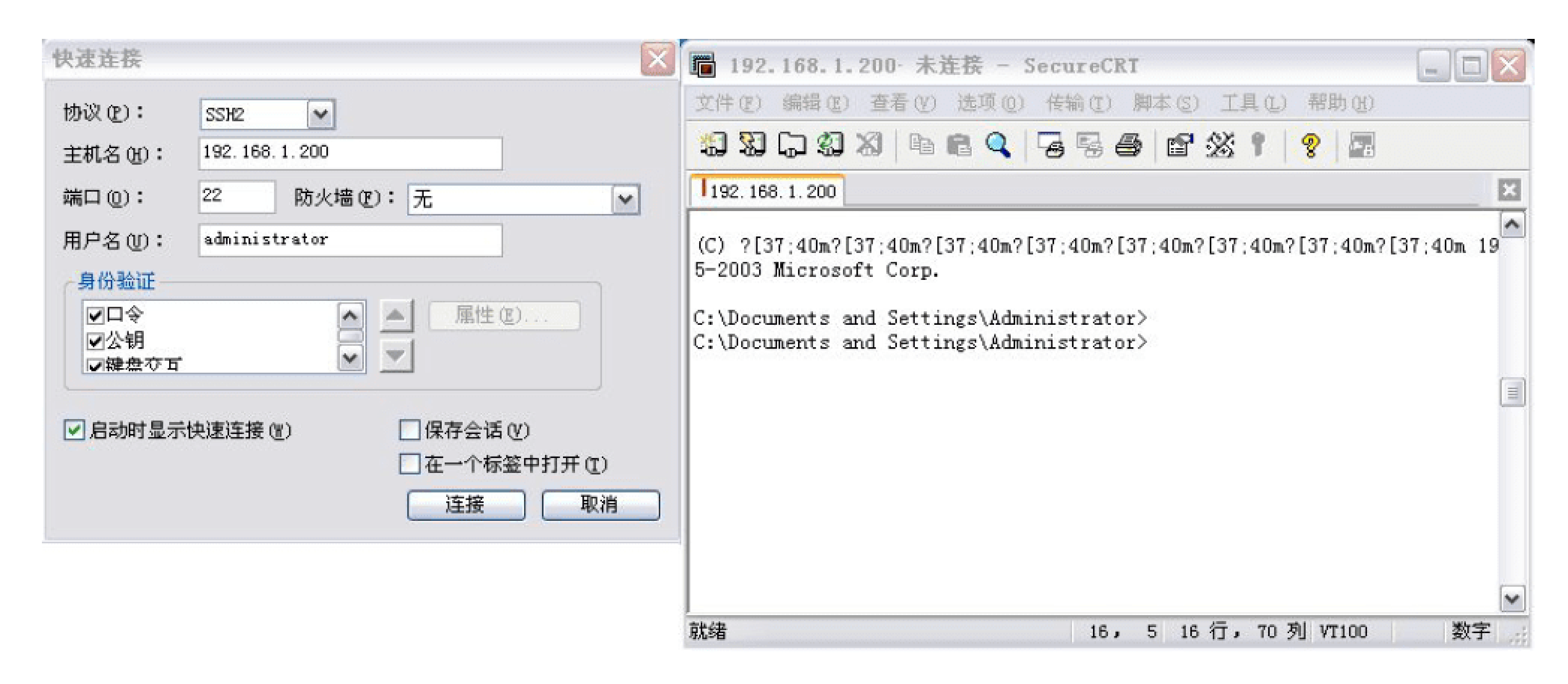


图 3-52　SSH 方式远程登录 Windows 主机

3.2.6　ARP 和 RARP 协议

ARP（Address Resolution Protocol，地址解析协议）用于将计算机的 32 位 IP 地址转换为 48 位的物理地址，其官方说明文档是 RFC 826。

RARP（Reverse ARP，反向地址解析协议），用于将网卡物理地址（MAC 地址）转换到对应的主机 IP 地址。RARP 协议客户端通过自身的 MAC 地址，向路由器 RARP 服务器请求 IP 地址。由于该协议自身的缺点，已被 DHCP 协议所取代。

1. ARP 协议的原理

当两台主机设备进行数据通信时，无论双方经过何种方式建立连接，例如经过局域网还是广域网连接，使用何种协议和加密机制，最终数据都要经过网卡物理接口来发送和接收数据，所以网卡的 MAC 地址非常的重要。但是，在主机传递数据包时，只知道对端 IP 地址，并不知道对端主机的 MAC 物理地址，所以需要 ARP 和 RARP 协议负责担任 IP 地址与 MAC 地址之间的对应和转换，并最终将数据包发送到指定的网卡接口。

注意：两台主机处于同一局域网进行数据通信时，ARP 协议可直接获取对方主机的 MAC 地址，并将数据传送至该 MAC 地址；处于不同的局域网时，ARP 协议将获取路由器作为数据出口的 MAC 地址，所有数据经过该 MAC 地址转发出去，最终发送至目标主机。

针对 ARP 协议，存在一种专门的攻击手段，即 ARP 攻击。ARP 攻击通过伪造 IP 地址和 MAC 地址的对应关系，从而造成数据发送失败或被恶意篡改，或者生成大量的 ARP 信息，造成网络的拥塞。

遭受 ARP 木马攻击，最常见的现象就是频繁的网络时断时续。防止 ARP 攻击，可采

用建立静态 ARP 缓存表的方式解决，或者绑定主机 IP 地址和 MAC 地址，甚至同时绑定交换机的端口。请参考本书第 2 章的交换机 IP 地址绑定部分讲解。

2. ARP 协议的应用

为了实现 IP 地址和 MAC 地址之间的对应关系，主机维护着一张重要的数据表，即 ARP 缓存表。当某主机在发送数据到目的 IP 地址时，首先查找 ARP 缓存表，如果能够找到对端 MAC 地址，那么直接发送数据。如果无法找到对端 MAC 地址时，该主机会发送广播数据包进行询问，对端主机接收广播后，回复自己的 MAC 地址。

由于 ARP 协议会自动维护和更新 ARP 缓存表，除非预防或解决 ARP 攻击，否则通常不会有 ARP 协议的具体应用。在 Windows 操作系统中，可通过 Arp –a 命令查看 IP 地址与 MAC 地址的对应关系。ARP 缓存表如图 3-53 所示。

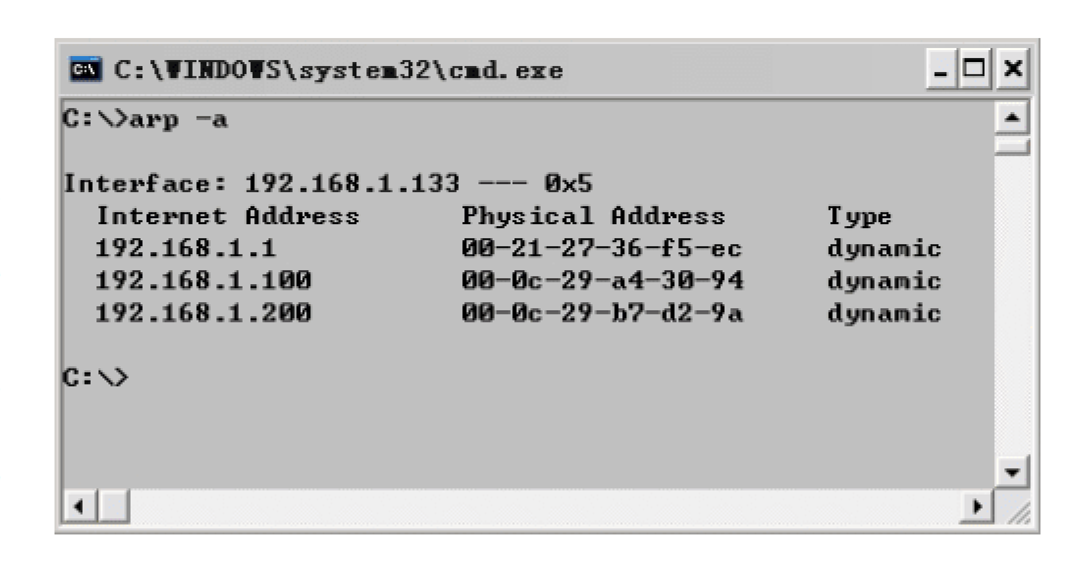


图 3-53　在 Windows 系统中查看 ARP 缓存表

同样，在 Redhat Linux 系统中也有该命令，执行结果如图 3-54 所示。

```
[root@RedhatServerroot]#arp -a
? (192.168.1.1) at 00:21:27:36:F5:EC [ether] on eth0
? (192.168.1.133) at 00:1D:72:80:1B:DE [ether] on eth0
? (192.168.1.200) at 00:0C:29:B7:D2:9A [ether] on eth0
[root@RedhatServerroot]#_
```

图 3-54　在 Linux 系统中查看 ARP 缓存表

3.2.7　POP3 和 SMTP 协议

SMTP（Simple Mail Transfer Protocol，简单邮件传输协议），使用 TCP 端口 25。SMTP 协议是一种发送邮件的协议，其定义了 E-mail 从源地址发送至目的地址的规则，为用户提供了可靠、安全、快捷的邮件传送服务。SMTP 协议可以控制邮件从客户端发送至服务器，也可以实现邮件从服务器传送到另一个服务器，最终送达目的邮箱地址。

POP3（Post Office Protocol 3，邮局协议的第 3 个版本），使用 TCP 端口 110 。POP3 协议是一种接收邮件的协议，其定义了客户端从远程服务器上接收邮件并保存至本地主机的规则，使得主机不需要实时与邮件服务器保持连接，减轻了服务器的负载。

除了 SMTP 和 POP3 协议之外，还有一系列的协议系统提供邮件服务，例如邮件存储、路由转发、兼容等服务。本书的后续章节中将详细介绍邮件服务器相关的服务协议，以及如何通过网管程序对各协议进行监测。此处简单介绍 SMTP 和 POP3 协议。

在 Windows Server 2003 操作系统中安装了 Exchange 服务程序后将生成服务进程，要确保邮件服务正常运行，就需要确保服务进程的启动。在控制面板中，选择【管理工具】|【服务】选项，在列表中选择 SMTP 服务，可查看该服务的运行状态，如图 3-55 所示。

选择 Microsoft Exchange POP3 服务，可查看 POP3 服务的运行状态，如图 3-56 所示。



图 3-55　邮件服务器上的 SMTP 服务状态

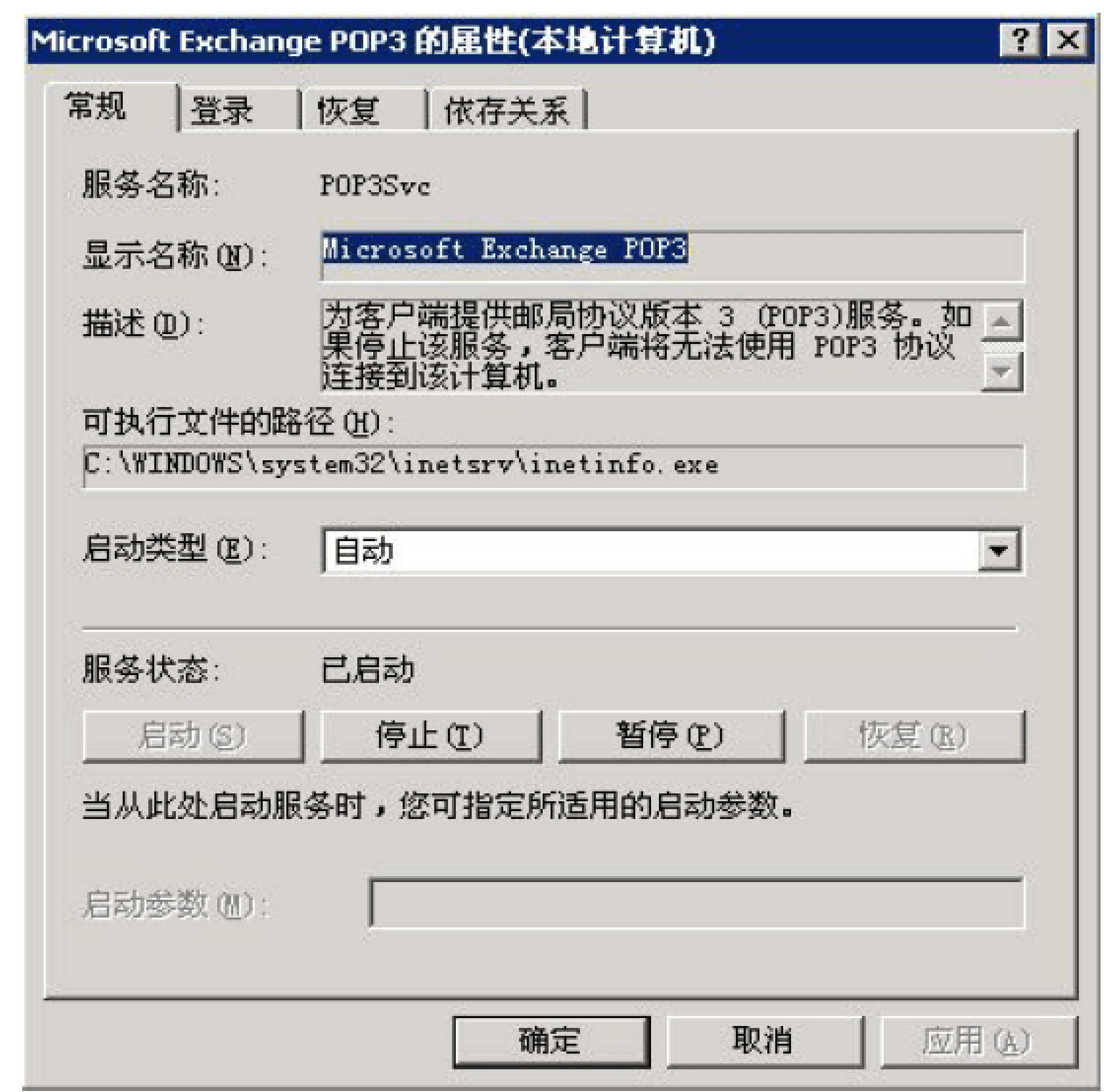


图 3-56　邮件服务器上的 POP3 服务

除此之外，邮件服务器还需要相关的一系列协议提供其他协作服务，从而共同完成电子邮件传递的功能。例如，IMAP 协议、Management 服务等，这些都是邮件服务器中的必要服务，如图 3-57 所示。



图 3-57　邮件服务器所需的相关服务

如果要对以上协议或服务进行具体配置，可选择【Exchange 系统管理器】，并选择【服务器】|【本地邮件服务器名】|【协议】目录，该目录提供了对相关邮件协议的具体配置，如图 3-58 所示。



图 3-58　Exchange 系统管理器中可对协议进行配置

3.2.8 DNS 协议

DNS（Domain Name System，域名系统）协议，是 TCP/IP 协议族的子协议，其主要功能是实现 Internet 互联网中域名与 IP 地址的翻译。例如，将域名 www.china.com 翻译为 IP 地址 222.194.139.60。通过 DNS 的域名解析功能，用户可以直接输入简明易懂的域名直接访问网络，而不用通过难以记忆的 IP 地址访问网络资源。

在互联网中，每一个域名都有一一对应的 IP 地址。在访问资源时，DNS 服务首先查找到指定域名对应的 IP 地址，再根据该 IP 地址连接到互联网服务器。

1. 客户端设置 DNS 服务器地址

在 Windows 客户端操作系统中，要通过域名（Web 地址）正常访问互联网 Web，而本地并未提供域名解析服务，那么就需要设置一个为本地主机提供域名解析的服务器地址，即 DNS 服务器的地址。

在 Windows XP 系统中，打开【网络连接】|【本地连接】的快捷菜单。选择【属性】选项，然后双击选择【Internet 协议（TCP/IP）】，将弹出 TCP/IP 属性配置界面。在界面中可设置 DNS 服务器的地址，此处的 202.103.224.68 是广西提供的公共 DNS 服务器地址，如图 3-59 所示。

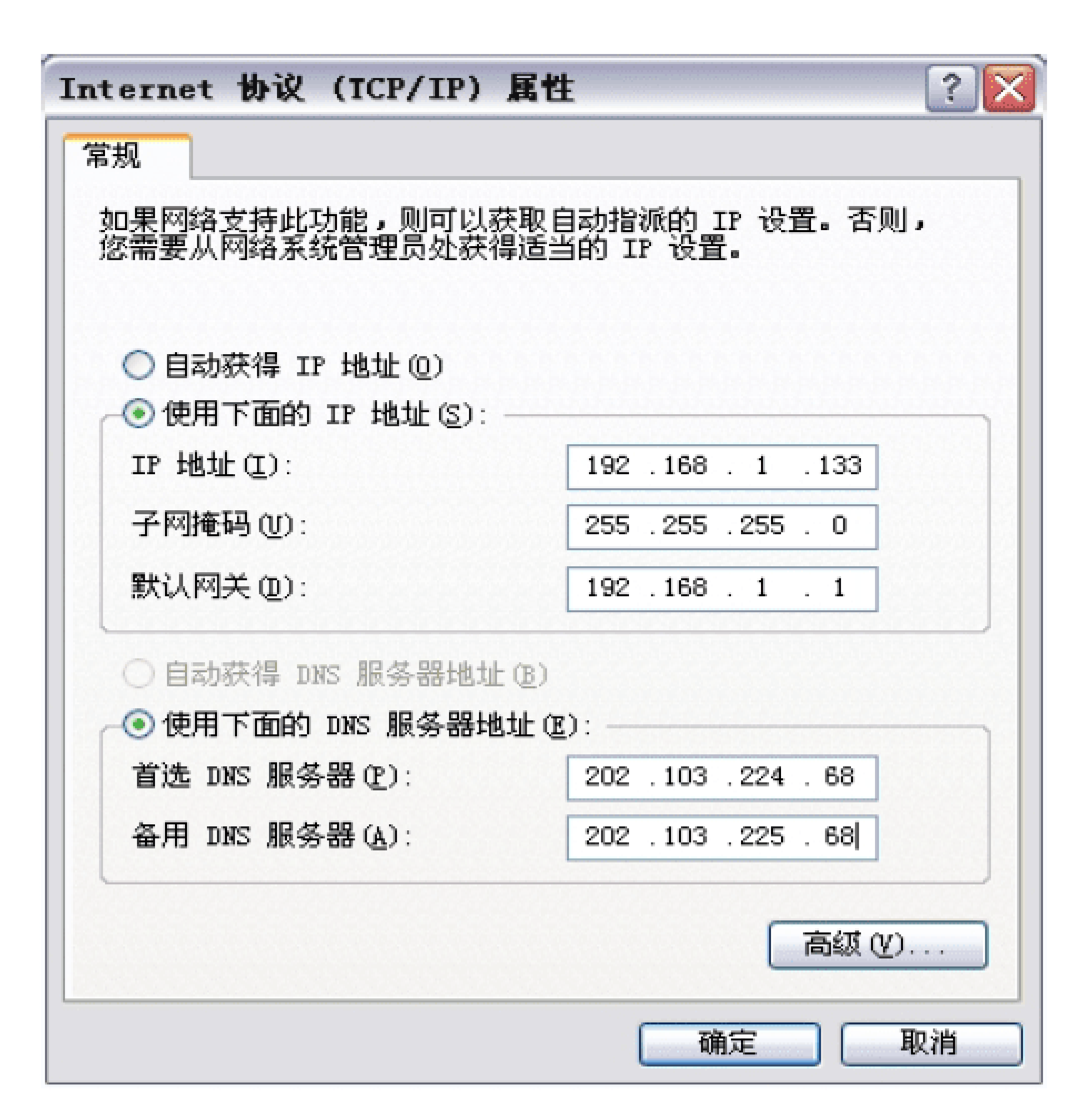


图 3-59 设置客户端 DNS 服务器地址

如果在本地主机中已接入互联网，但取消该 DNS 服务器地址，则在 Web 页面中输入域名将无法正确访问该网站，但却可以 Ping 通该 Web 站点所使用的 IP 地址。也就是说，网络是畅通的，但没有域名解析服务。

注意：该 DNS 地址可以设置为公共的 DNS 服务器地址，也可以使用局域网中专门提供 DNS 解析的服务器地址。

2. 服务器端设置 DNS 服务

Windows XP 未提供 DNS 解析服务功能。但在 Windows Servers 版本中，如 Windows Server 2000/2003/2008 系统中，均提供了 DNS 服务组件。选择【控制面板】|【添加\删除 Windows 组件】选项，在打开的 Windows 组件安装界面中选择【网络服务】|【域名系统 DNS】选项，即可进行该组件的安装，如图 3-60 所示。

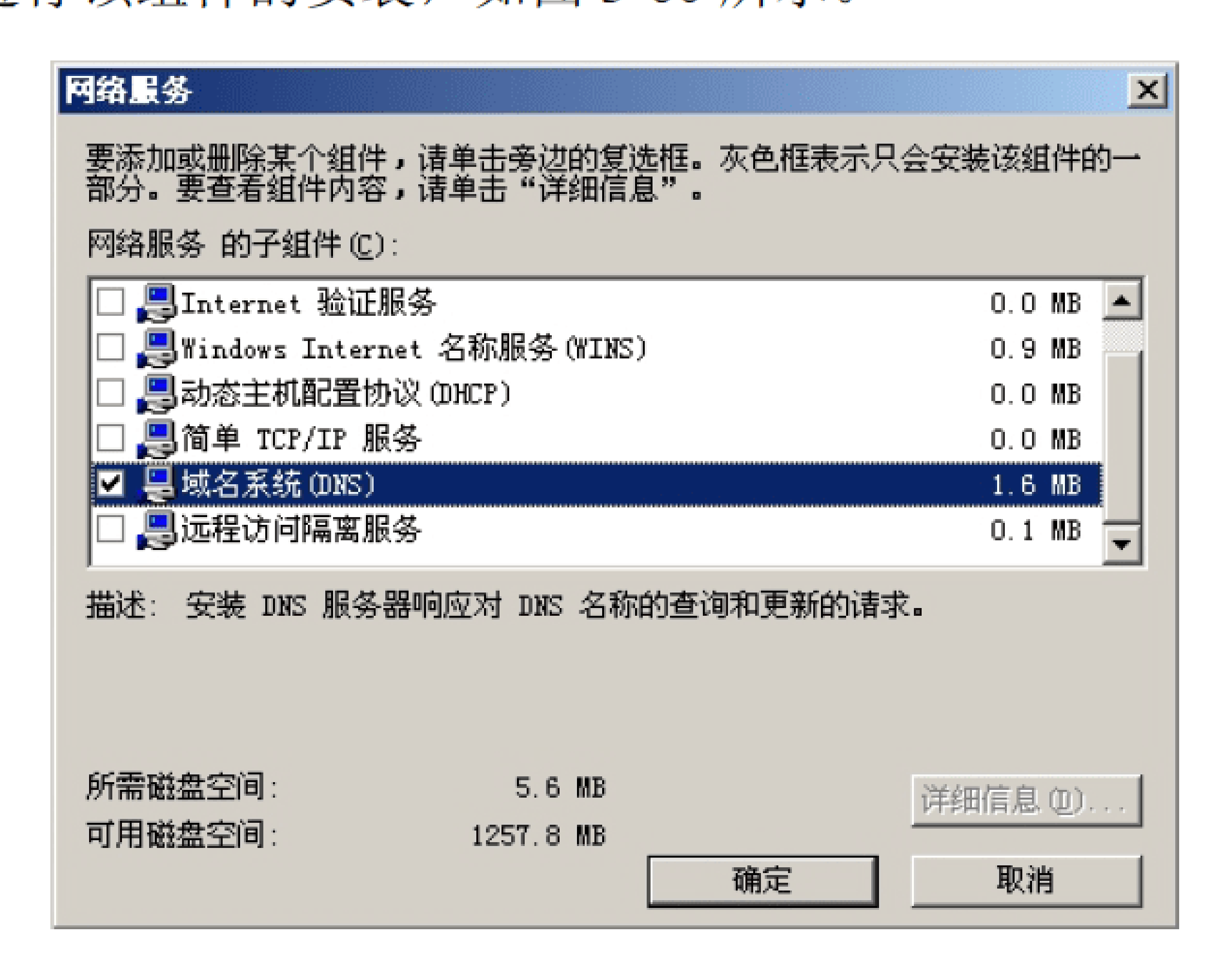


图 3-60　在 Windows Server 2003 系统中安装 DNS 服务组件

安装 DNS 组件后，即可在开始菜单中选择 DNS，对其进行配置，配置界面如图 3-61 所示。

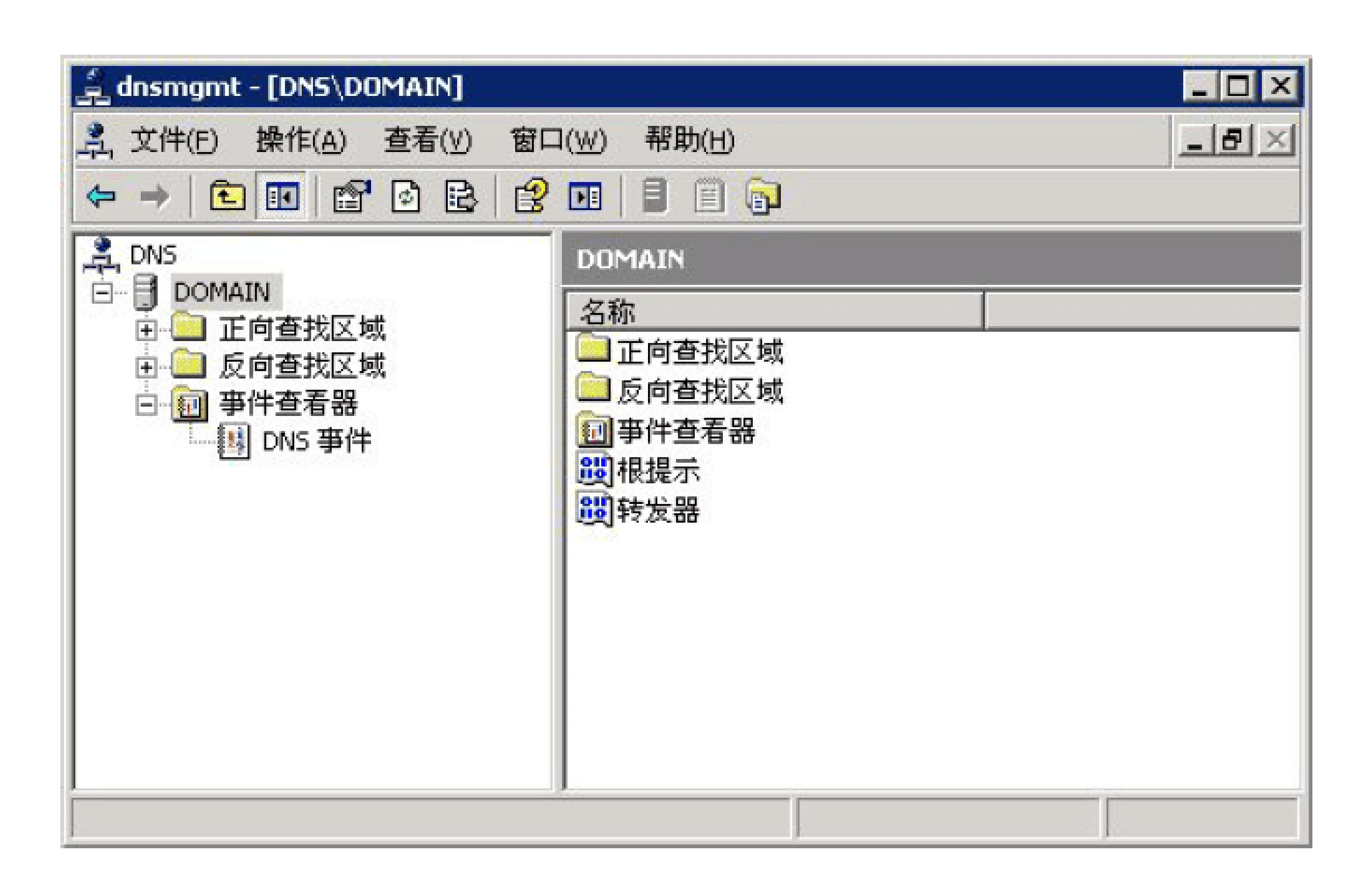


图 3-61　服务器的 DNS 配置界面

DNS 的详细配置请查阅相关资料，此处介绍两个重要的配置项。

- 正向查找区域：当用户请求解析某域名时，在该区域查找域名对应的 IP 地址，并返回 IP 地址信息。
- 反向查找区域：当用户请求解析某 IP 地址，在该区域查找对应的域名，并返回域名信息。

同样，在 Redhat Linux 系统中也提供了 DNS 域名解析服务。在安装 DNS 服务组件后，可在主菜单中选择【系统设置】|【服务器设置】|【域名服务】选项，打开 DNS 配置界面，如图 3-62 所示。

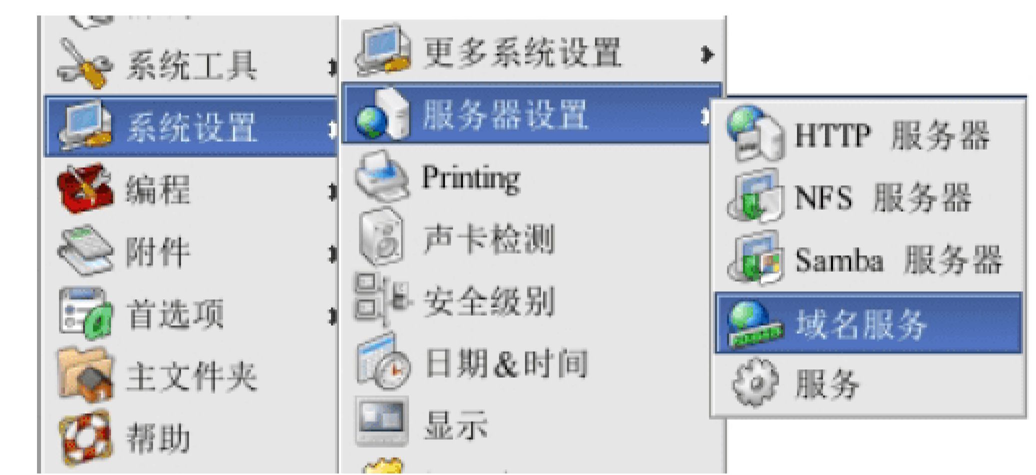


图 3-62　在 Linux 系统中选择设置 DNS 域名服务

3. DNS 服务的测试

如果要测试 DNS 服务器域名解析功能是否正常，可使用 Nslookup 命令。该命令最简单的使用方式就是查询一个 Web 域名所对应的 IP 地址，以及通过 IP 地址查询域名信息。如果能够正常解析到二者的对应关系，则说明 DNS 服务器工作正常。

例如，使用该命令解析 Web 服务 www.baidu.com，命令格式为 Nslookup [域名]，命令执行结果如图 3-63 所示。



图 3-63　Nslookup 命令查看域名解析服务

此时看到该 Web 站点对应的互联网 IP 地址为 202.108.22.5 和 202.108.22.142，就能够说明该站点域名解析服务正常。如果返回的内容是：

```
*** Can't find www.baidu.com : Non-existent domain
```

那么说明 DNS 服务器的域名解析服务不正常。

在测试了域名解析后，通常还要监测反向域名解析服务，即通过 IP 地址是否能够正确解析到域名，命令格式为 Nslookup [IP]。同样解析 Baidu 站点的 IP 地址，命令如图 3-64 所示。

此时可看到，该地址能够解析出该站点的域名，反向解析服务同样正常。

注意：Nslookup 命令是 TCP/IP 协议自带的检测工具。在 Linux 系统中同样可以使用该命令。



图 3-64　Nslookup 命令查看反向域名解析服务

3.2.9 SNMP 协议

SNMP（Simple Network Management Protocol，简单网络管理协议），定义了一种从网络中的设备节点上获取网络管理信息的方式。目前各类网络设备和主机设备都提供了对SNMP 协议的支持，绝大部分的网络管理程序也是通过 SNMP 协议实现网管功能。

要通过 SNMP 协议实现对路由器、交换机、Linux 主机或 Windows 主机进行状态监测，首选需要安装或开启被监测设备中的SNMP服务。如果想要获取设备在出现故障或异常时，主动报告网管系统的信息，那么还需要在被监测设备中开启 SNMP Trap 服务。例如，某Windows XP 主机，如果需要通过网管程序远程获取该主机的运行状态，那么需要在Windows XP 主机中安装和开启 SNMP 服务，且进行相关的配置。

有关 SNMP 协议的结构、特征，以及如何在各类设备和系统中安装、开启、配置 SNMP服务，将在后续章节中进行详细的介绍。后续的网管工具介绍也都是通过 SNMP 协议实现网管功能，此处仅作为协议介绍的一部分进行简单说明。

3.2.10 IPX/SPX 协议

IPX（Internetwork Packet Exchange，网间数据包交换），该协议由 Novell 公司开发，负责实现在 Novell NetWare 网络中数据包的交换，但并不保证数据的可达和准确性。

SPX（Sequences Packet Exchange，顺序包交换），同样是由 Novell 公司开发的一种用于局域网的网络协议。在 NetWare 网络中，SPX 协议主要负责完成对数据包的纠错。

IPX/SPX 协议的特点是，通过该协议实现网络互联并不需要进行设置。该协议提供了路由和寻址功能。Novell 网络中的每个节点都有唯一的网络地址，由两段组成，前一段地址是网络标识，存储于 NetWare 服务器。而后一段地址是节点网卡的 ID 标识，组成了节点唯一的网络地址。所以在使用 NetWare 时，不需要对 IPX/SPX 协议进行配置。

IPX/SPX 是专门用于 NetWare 网络的通信协议。由于采用 IPX/SPX 实现节点间的互联不需要任何设置，目前在一些大型的联机游戏中采用 IPX/SPX 协议实现互联。但在 TCP/IP协议的网络中，不会使用该协议。

注意： *用户接入 Novell NetWare 网络时，最好采用 IPX/SPX 协议，以确保更好的兼容性。*

要在 Windows 系统中安装 IPX/SPX，可打开【本地连接】的快捷菜单，选择【属性】菜单命令，在弹出的配置界面单击【添加】按钮，并依次选择【协议】|【NWLink IPX/SPX/NetBIOS】选项，进行 IPX/SPX 组件的安装，如图 3-65 所示。

3.2.11 TCP/IP 协议

TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议）中的。TCP 和 IP 协议是两个紧密结合的协议，二者已经发展成为互联网中最基础、最重要

以及应用最广泛的协议，它也是唯一能够承载 Internet 网的基础架构协议。TCP/IP 协议不仅仅是两种协议，而是代表了一组协议。



图 3-65　在 Windows 系统中安装 IPX/SPX 协议

其中，TCP 协议为数据传送协议，而 IP 协议则为每一台网络中的设备定义了唯一的身份标识，以及负责数据的发送和接收等。那么，有了数据传送的起点和目的地，以及数据传输过程中的控制，便能够实现数据的交互。

注意：TCP/IP 协议并不是简单的两个协议，而是代表了一组协议，其中包括常见的 Telnet、FTP、HTTP、POP3 协议等。

1．TCP/IP 的特点及发展历史

TCP/IP 协议的特点如下：

- TCP/IP 协议能够适应和支持不同的网络结构，能够在互联网、局域网、广域网、等不同的异构网络结构中得到广泛应用。
- TCP/IP 协议不依赖于任何操作系统或硬件设备，是一个开放性的协议，支持各类硬件设备，如计算机、网络设备、环境动力配套设备等。
- 使用全球通统一的网络地址分配方案，使得网络中的每一个节点都有一个唯一标识自己的 IP 地址。

TCP/IP 协议的发展历史如下：

- 1970 年，Internet 网络的前身 ARPANET 网开始使用网络控制协议（NCP）进行网络互联，该协议是传输控制协议（TCP）的雏形。
- 1981 年，Internet 协议（IP 协议，即 IPv4 版本）出现，ARPANET 朝着 Internet 互联的方向快速发展。
- 1982 年，国防通信署（DCA）和 ARPA 组织规定了 TCP 协议和 IP 协议作为协议套件，称为 TCP/IP 协议，为网络提供可靠的、可寻址路由的传输。

❑ 1996年，Internet协议第二版本IPv6标准发布。

之后，TCP/IP协议得到不断的改进和发展，完全取代了NCP协议，并随着Telnet、FTP、DNS、HTTP 等协议的出现，发展成为能够支持异构网络、支持各类系统和硬件、广泛支持各类应用协议的标准连接协议。

2．TCP/IP协议的安装

TCP/IP协议定义了在互联网或私有网络中的一整套协议组件。其中，IP协议是该组件中最为核心的协议，它定义了Internet网使用IP地址作为节点的唯一标识。IP协议包括IPv4和IPv6两个版本，目前流行的是IPv4版本。但为了解决IPv4地址资源枯竭的情况，在1996年推出了IPv6版本。该协议可提供数量庞大的地址，满足可预计未来的使用。但IPv6还需要操作系统、硬件设备、网络程序、网络协议等组件的匹配和支持，所以，IPv6仍在不断推进建设和投入实际应用的过程中。

注意：IPv4采用32位地址，可分配约43亿个地址。而IPv6采用128位长，可提供几乎无限制长度的数量。

安装Windows操作系统时，默认安装了TCP/IP组件，使用的是IPv4的地址。也可选择安装IPv6版本，IPv6不会影响当前网络的运行，且在安全认证机制、网络诊断支持、网上邻居检测、数据转发效率等方面均有所增强。在Windows操作系统中，IPv6组件称为“Microsoft TCP/IP 版本 6”，可选择安装或者卸载。

在Windows XP操作系统中的【网络连接】|【本地连接】上打开其快捷菜单，单击【属相】|【常规】页面的【安装】按钮，将进入网络组件安装选择界面。分别选择【协议】选项和【添加】按钮，在弹出的组件界面中安装Microsoft TCP/IP 版本 6即可，如图3-66所示。

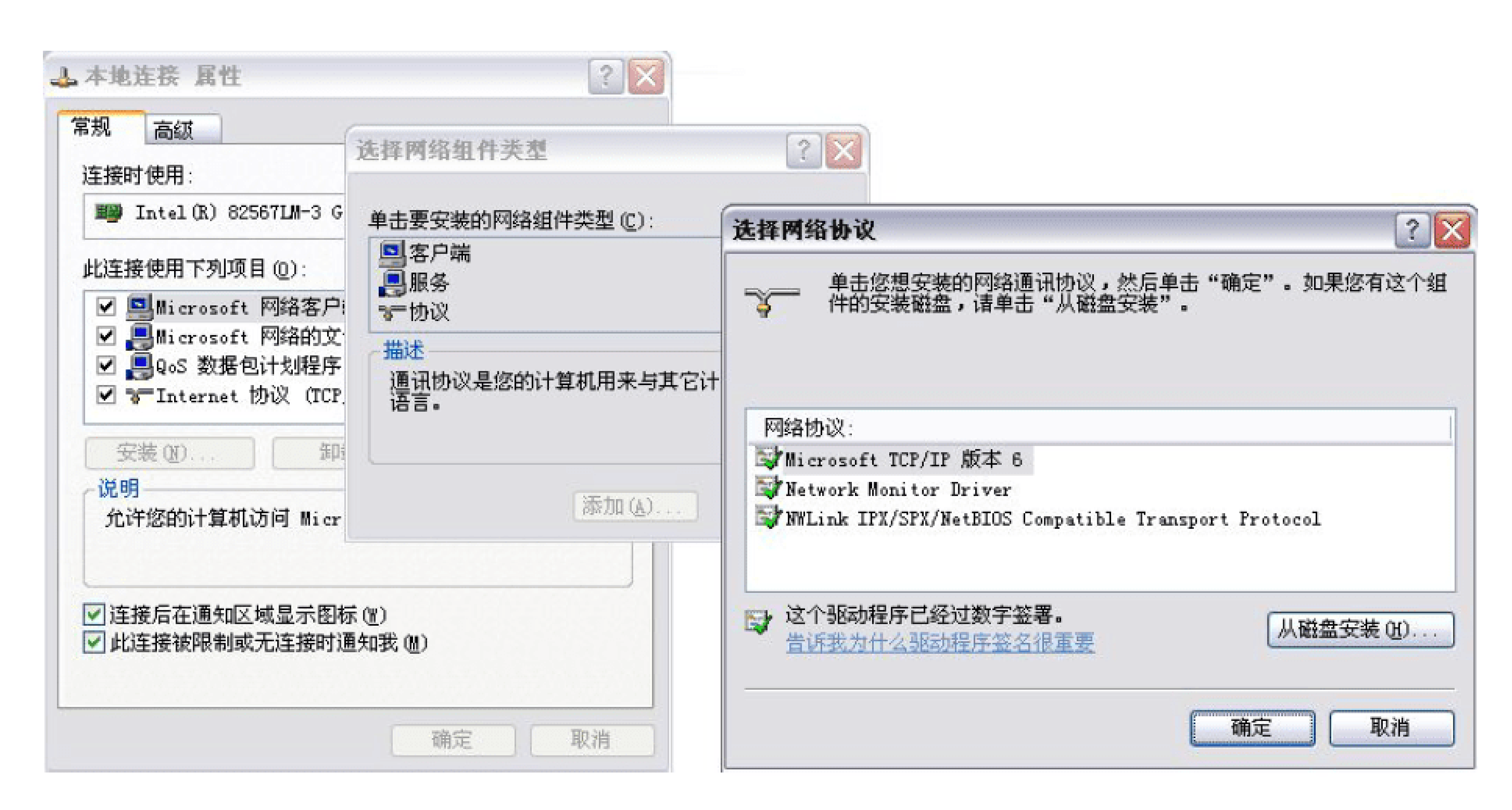


图3-66　安装TCP/IP协议的IPv6版本

如果需要卸载该协议，可在本地连接的属性界面选择【Microsoft TCP/IP 版本 6】选项，之后单击【卸载】按钮即可，如图3-67所示。

TCP/IP 版本 6 支持系统自动配置 IP 地址。在 IPv6 协议启动后，将会发送一条请求消息进行本地路由器的查找，路由器在接收到请求信息后进行响应，IPv6 主机根据响应信息自动分配 IPv6 地址。如果需要手动配置 IPv6 地址，可在命令提示符界面使用命令 netsh interface ipv6 命令下的子命令进行操作。



图 3-67　卸载 TCP/IP 版本 6

3．TCP/IP 协议诊断工具列表

在安装 TCP/IP 协议后，系统中将包含一系列用于测试 TCP/IP 服务的诊断工具。维护人员在网络维护过程中将会经常用到这些简单而实用的测试工具，见表 3.3。

表 3.3　Windows 系统 TCP/IP 协议常用诊断工具列表

序号	工具名称	描　述
1	Ping	最常用的测试网络的连通工具，Ping 对方主机名或 IP 地址即可。Ping 127.0.0.1 是测试本地循环地址，如果无法 Ping 通，则表明本地 TCP/IP 协议工作不正常
2	Ipconfig	查看本地 TCP/IP 协议的配置信息，最常用的是 Ipconfig /all、Ipconfig /renew（更新自动获取的 IP）、Ipconfig /release（释放自动获取的 IP）、Ipconfig/flushdns（刷新和释放 DSN 缓存信息）
3	Netstat	显示基于 TCP/IP 协议的网络连接状态。常用的是 Netstat –a 命令，查看连接至本地计算机的连接状态
4	Arp	查看 IP 地址与网卡物理地址对应关系表。常用的是 Arp –a 命令
5	Nslookup	用于测试 DNS 服务器能否正确实现域名解析的工具。通常使用 Nslookup [域名]查看是否将域名正确解析为 IP，或使用 Nslookup [IP]命令查看反向解析是否正确
6	Tracert	跟踪 IP 数据包发送至目的地址的路径
7	PathPing	该命令结合了 Ping 和 Tracert 命令，用于测试数据包发送至目的地址的路径，以及在发送过程中的丢包情况
8	Route	查看、删除和添加路由表信息

4．Linux 系统的 TCP/IP 协议

此处以 Redhat Linux 9 系统为例，简单介绍在 Linux 系统中，TCP/IP 协议中的 IP 地址的配置。

在 Redhat Linux 系统的图形界面中选择主菜单命令【系统设置】|【网络】，在弹出的配置界面中将看到名为 eth0、eth1 或更大编号的网卡设备列表。双击要编辑的网卡即可弹出 IP 地址设置界面，可设置自动获取 IP 或手动设置 IP 地址，类似于 Windows 系统中的 IP 地址设置，如图 3-68 所示。

在 Redhat Linux 系统中还包含多个 TCP/IP 协议相关的网络配置文件，这些文件分别提供了不同的网络服务。其文件名称、路径及内容见表 3.4。

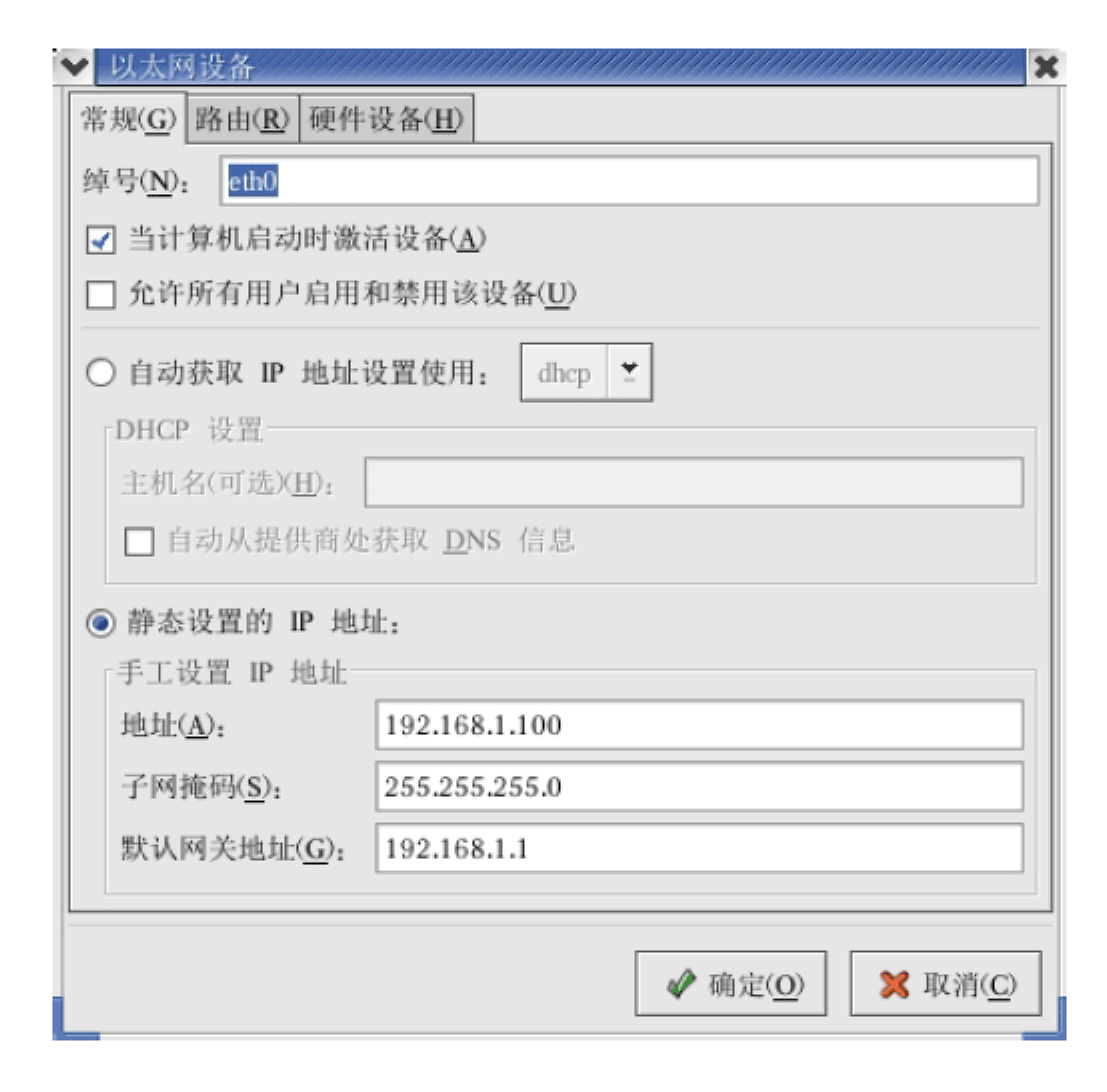


图 3-68　设置 Redhat Linux 系统中的网卡 IP 地址

表 3.4　Redhat Linux 系统中的 TCP/IP 协议相关的网络配置文件列表

序号	文 件 名 称	配置文件内容
1	/etc/resolv.conf	包含 DNS 服务器地址、域名解析服务配置等信息
2	/etc/sysconfig/network	用于指定服务器的网络配置信息，包含主机名、网关等内容
3	/etc/sysconfig/network-scripts/ifcfg-<Id>	网卡配置文件，其中 Id 代表网卡的序号，Ifcfg-eth0 是第一块网卡配置文件，Ifcfg-eth1 是第二块，其中包含了网卡的 IP 地址、掩码、网关等信息
4	/etc/hosts	包含主机名与 IP 地址对应关系的信息
5	/etc/hosts.conf	用于指定主机名解析的方式，如指定查询顺序、防止 IP 欺骗等
6	/etc/protocols	包含当前系统可用的协议
7	/etc/vsftpd/vsftpd.conf	用于配置 Vsftp 服务，包括开启 FTP 服务、配置是否允许匿名登录等
8	/etc/xinetd.d/telnet	用于配置 Telnet 远程登录服务，内容包括开启服务、设置端口、服务限制等
9	/etc/ssh/ssh_config	用于配置 SSH 远程登录服务，内容包括允许登录用户列表、是否运行图像转发等内容

3.3 本章小结

本章主要介绍了计算机网络中涉及的重要协议。在对各协议的发展历史、功能特点进行讲解的基础上，更侧重对协议的管理和简单应用的介绍，以加深读者对网络协议的理解和应用。

本章介绍的网络协议知识对于后续章节中的网络管理和监测知识而言非常重要，是学习网络监测技术必不可少的基础知识，网络管理员应重视对网络协议的学习。

第 4 章　SNMP 和 WMI 知识介绍

要了解网络运行方式，用好网络监测工具管理网络，就需要了解网络管理的基础架构和原理。SNMP（Simple Network Management Protocol，简单网络管理协议）体系结构涵盖了网络管理中必不可少的基础性结构、协议和组成部分，学习和掌握 SNMP 的相关知识对于后期理解网络监测、管理和优化技术非常重要。本章介绍 SNMP 体系的相关知识。主要内容如下：

- SNMP 体系结构简介及组成部分。
- SNMP 协议、SMI（Structure of Management Information，管理信息结构）、MIB（Management Information Base，管理信息库）的原理、结构和应用。
- 各类设备和系统中 SNMP 服务的配置和应用。
- WMI 体系和应用。

本章涉及较多的网络基础概念，书中将会通过一些实际操作加深对这些理论知识的理解。

4.1　SNMP 体系实体组成部分

在介绍 SNMP 体系结构之前，首先介绍该体系结构中涉及的实体组成部分，后续的内容将用到这些概念。SNMP 网络包括 3 个关键组成部分：管理者、被管理者、管理代理。以下分别介绍该 3 个组成部分：

4.1.1　SNMP 管理者（SNMP Manager）

SNMP Manager 就是运行 SNMP 网管系统的管理主机，用于协助网络管理员完成整个网络管理工作。管理主机将请求信息或配置信息命令发送到被管理主机中的 SNMP 代理程序，要求 SNMP 代理收集重要的设备信息或更改设备配置，以确定和更改独立设备或整个网络的运行状态。同时，管理主机应该定期查询 SNMP 代理收集到的有关主机运转状态、配置及性能等信息。

SNMP 管理者通过 GET、GETNEXT 和 GETBULK 等协定指令取回信息，也可以传送配置更新或控制请求，通过 SET 协定指令送达到被管理设备中。

4.1.2 被管理的设备（SNMP Managed device）

一个被管理的设备是一个存在于SNMP网络中的节点，这些节点均包含SNMP代理程序。被管理的设备会通过MIB（管理信息库）收集和存储管理信息，并通过SNMP代理使网络管理系统获取这些信息。被管理的设备有时被称为Network Elements（网络元素），可以是路由器、服务器、交换机、网桥、主机或打印机等。

4.1.3 SNMP代理（SNMP Agent）

SNMP代理是一种存在于被管理的设备中的网络管理软件模块，担任着管理主机与被管理设备之间的信息交互中介。SNMP代理通过控制设备的管理信息数据库（MIB）来管理设备信息，并拥有本地设备（网络设备、工作站、服务器等）各类信息。这些信息包括被管设备的运转状态、设备特性、磁盘空间使用、系统负载、系统配置等相关信息。

代理在没有被网管主机询问的情况下，也可主动发送TRAP（陷井信息）或INFORM（通知信息）给网管主机。SNMP TRAP被用于被动形式的网络监控，即网管主机不主动请求和控制，当有异常状态触发报警时，SNMP代理通知网管主机。

三者的关系可以用图4-1进行表示。

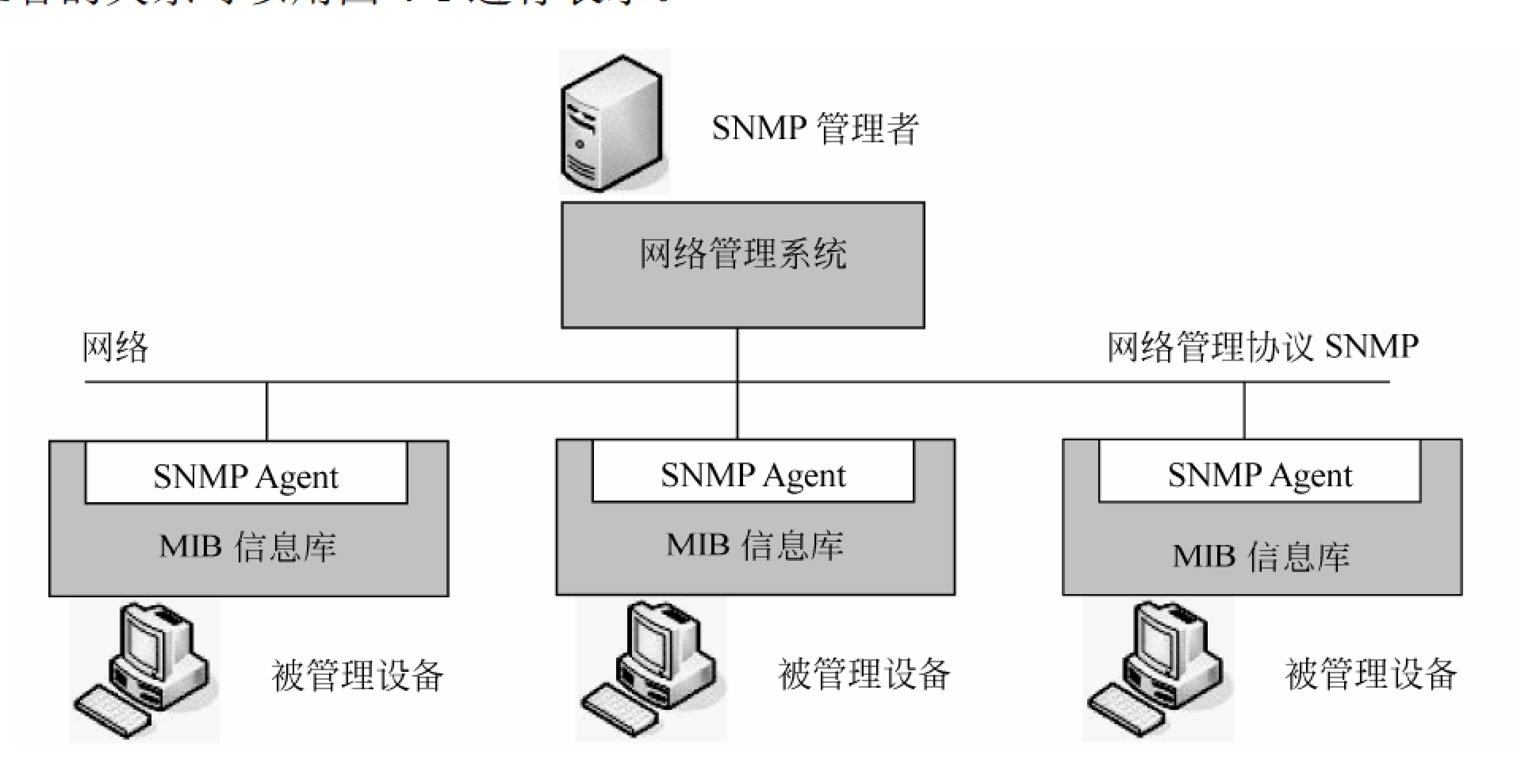


图4-1　SNMP网络组成部分

在对网络组成实体进行简单介绍后，将对SNMP的理论体系结构进行详细描述。4.2节将介绍体系结构中最为重要的SNMP协议。

4.2 SNMP体系系统结构

SNMP体系的系统结构包含3个系统组成部分：SNMP协议、SMI（管理信息结构）和MIB。SNMP协议提供了底层网络管理的整体框架，定义了SNMP网络遵循的统一协定

和规范；SMI 则定义了网络信息对象的存储、管理的相关规范；而 MIB 详细的定义了每一个 SNMP 信息对象的内容、属性和操作。

下面首先对 SNMP 协议进行介绍。

4.2.1 SNMP 协议概述

简单网络管理协议 SNMP 是由 IETF（Internet Engineering Task Force，互联网工程工作小组）所定义。它是 Internet 协议族的一部分，被广泛应用在 NMS（Network Management System，网络管理系统）及诸多种类的网络设备、软件和操作系统中。

SNMP 协议的设计目标是对众多厂家生产的不同软硬件建立一个通用的管理平台。该平台不依赖于具体的设备、系统和网络传输协议，且具备独立性和可扩充性，以及能够更充分地利用远程管理和 Internet 资源，实现各种网络设备间方便的信息传递，同时通过一定安全访问机制，保证网络安全性。基于上述设计原则，SNMP 的出现，为网络管理系统提供了底层网络架构的通用框架，极大地简化了网络设备的管理和维护工作，通过 SNMP 管理网络，能够让网管员全面了解网络运行状态、设备性能，及时发现和排除网络故障。

SNMP 协议是基于 TCP/IP 协议一个应用层协议，它使用传输层上面向无连接的 UDP（User Datagram Protocol，用户数据包协议）传输协议，并使用端口 161 和 162 进行通信。

4.2.2 SNMP 版本及发展

SNMP 开发于 20 世纪 90 年代早期。其最初的目的是简化网络设备的管理和数据的获取。随着 SNMP 的不断发展，它被应用到各种网络管理系统中，并开始受到各类硬件厂商的广泛关注和支持。厂商在每个硬件设备中都加入了对 SNMP 协议的支持，从交换机、防火墙到路由器和服务器，从 Unix、Linux 到 Windows 操作系统，各类设备和系统都默认支持 SNMP 协议管理。

目前 SNMP 包括 3 个版本：SNMP v1、SNMP v2 及最新的 SNMP v3。

1990 年 5 月，RFC（Request for Comments“请求注解”，即互联网协议的草案及标准）定义了 SNMP 的第一个版本 SNMP v1。作为一种简单的请求/响应协议。即网络管理系统发出一个请求，管理器则返回一个响应。这一行为的实现是通过使用 4 种操作来完成，这 4 种操作命令分别是 GET、GETNEXT、SET 和 TRAP。NMS 通过 GET 请求获取一个或更多的对象值。通过 GETNEXT 操作，请求获取列表或对象列表中取出下一个对象参数值。通过 SET 操作更改对象的配置信息。TRAP 操作则是非请求类操作，NMS 不需要主动请求即可得到由 Trap 操作所报告的特定事件信息。

1993 年 RFC 发布了 SNMP v2 版本。v2 版本除了支持 v1 中的 4 种操作，还定义了两种新的操作，即 GET BULK 和 INFORM 操作。NMS 通过 GET BULK 操作能有效地获取大块数据，可获得对象列表中尽可能多的信息。INFORM 操作使得一个 NMS 能发送 TRAP 给另一个 NMS 并能收到回复。

1998 年 1 月提出了互联网建议 RFC 2271-2275，既 SNMP v3 版本。v3 版本与前两种

版本相比，加强了在安全管理方式和远程控制方面的功能，并采用了新的 SNMP 扩展框架。安全性方面，SNMP v3 使用 DES（Data Encryption Standard，数据加密算法）加密数据通信，很大程度提高了 SNMP 的安全性。在当前的网络设备市场中，已经推出了多款支持 SNMP v3 的网络产品，在安全功能和管理功能上都有成功的应用。但目前较为通用的 SNMP 版本仍是 v1 和 v2 版本。

4.2.3 SNMP 协议的特点

SNMP 协议的应用范围非常广泛，主要是因为 SNMP 协议有如下特点：

- SNMP 协议最显著的特点就是其通用性。SNMP、MIB 及其他相关的体系框架能够在各种不同类型的设备上运行。包括个人计算机到高档的大型主机、服务器、及路由器、交换器等网络设备。甚至包括电话系统、环境控制设备，以及其他可接入网络的非传统网络设备。
- SNMP 管理易于实现，其设计简单，扩展灵活，同时提供完备的技术资料（例如 RFC 系列的资料和文档）供开发者参考和改进。
- SNMP 是开放的免费产品。

正是由于上述这些特点，SNMP 协议已经被认为是网络设备厂商、管理软件开发的首选管理协议。

但 SNMP 协议的通用性和扩展性同样带来了安全上的隐患。为了加强 SNMP 的安全性，在 SNMP v1 和 v2 版本中引入了通信字符串认证方式（也称为社区字符串）。许多厂商硬件设备中的 SNMP 服务都采用了该认证方式，这些认证字符串是管理程序获取设备信息和修改硬件配置的访问凭证（口令）。大多设备初始均配置了默认的社区字符串。最常见的默认值是 public（只读访问凭证）和 private（可读/写访问凭证）。也有许多厂商采用私有的默认社区字符串，但这些字符串均可根据用户需要自行更改。

虽然字符串认证方式的出现提高了 SNMP 的安全性，但 SNMP 仍较为脆弱。在 SNMP v1 和 v2 版本中，通信字符串和信息传递均采用明文的方式，其数据包容易被入侵者捕获，从而获取社区字符串，使网络面临入侵、信息篡改、信息泄露等威胁。在 SNMP v3 版本中，为保护通信字符串，使用了 DES、MD5（Message-Digest Algorithm 5，信息-摘要算法 5）和 SHA（Secure Hash Algorithm，安全散列算法）等加密和验证的新技术，进一步加强了安全性。

4.2.4 SNMP 协议报文和应用

SNMP 协议可按照两种方式来使用：轮询和陷井。轮询方式是网管程序最主要使用的方法，用于获取网络常用信息和监控设备状态。网管程序通过周期性地触发请求至终端设备的 SNMP 代理，这些请求为主动请求。如果设备响应了请求，则网管能够获取询问的信息。如果设备没有响应请求，则能够判断设备出现某种故障。SNMP 陷井能够被用来进行被动形式的网络监控，该方式通过配置 SNMP 设备的代理，让其在发生重要事件时报告网

管系统。在网管系统中同样包含了 SNMP 代理程序，并通过代理接收和处理陷井信息。

那么，SNMP 协议具体通过什么手段联系 SNMP 代理以获取对象信息呢？下面分别介绍 SNMP 操作命令类型、命令所发送的数据包格式和具体的数据包操作。

4.2.4.1 SNMP 协议报文格式

SNMP 命令也就是向对象发送数据包信息（也就是报文），由 3 个部分组成：版本信息（Version Field）、社区字符串（Community Field）和数据单元 PDU（Protocol Data Unit Field）。数据包的长度不是固定的，如图 4-2 所示。

版本标识符 Version	社区字符串 Community	数据单元 PDU

图 4-2　SNMP 协议数据包格式

版本信息：SNMP 版本信息，该信息的表述方式是版本号减 1。例如，SNMP v1 应写入 0，v2 版本则写入 1。目前较为通用的是 0 和 1。

社区字符串：也称为公共区、社区字符串，它是 SNMP 基本的安机制，用于访问 SNMP 代理时的认证口令。

协议数据单元 PDU：指明了 SNMP 报文的类型及相关参数，即 SNMP 提供的 3 类操作命令 Get、Set 和 Trap 之一。Get 为获取对象信息的请求报文，Set 为设置 MIB 数据对象报文，而 Trap 是代理主动发给管理者的报文信息。

4.2.4.2 SNMP 协议的操作应用

SNMP 协议提供了 3 类操作命令用于访问和控制 MIB 对象，分别是 Set、Get 和 Trap 操作，见表 4.1。

表 4.1　SNMP 协议的 3 类操作命令

命令	解　释
Get	该命令是 Read（读）命令，允许 SNMP 从与 Read 社区字符串匹配的网络设备中获取信息。该命令是获取设备管理信息的基本方式，也是使用率最高的一个命令。一般网络设备都默认具有“读”权限，默认字符串值通常为 public，作为管理进程和代理进程之间的明文口令
Set	该命令是 Write（写）命令，允许 SNMP 设置与 Write 社区字符串匹配的网络设备。它是一个特权命令，因为可以通过它来改动设备的配置或控制设备的运转状态。社区字符串一般默认是 private
Trap	Trap（陷井）信息是由被管理设备主动发出的信息，SNMP 允许接收与 Trap 社区字符串匹配的网络设备信息。它的功能就是在网络管理系统没有明确要求的前提下，由管理代理通知网络管理系统有一些特别的情况或问题发生了

以下举例介绍这 3 类操作。

1. Get 操作

网管系统想要获取被管理设备 MIB 节点 sysName（系统名称）的值，被管设备 SNMP

代理使用 public 作为社区访问字符串，那么操作过程如下：

NMS 给 SNMP Agent 发送 Get 请求，请求报文格式为 Version 字段(值为 2c)，Community 字段（值为 public），PDU 数据字段（值为 sysName.0）。

被管理设备的 Agent 收到 Get 请求后给 NMS 回复响应，如果 Get 操作成功，代理回应的数据字段值部分是设备的名字（如 PC-0021）。如果获取操作失败，则在“错误状态”字段填上出错的原因，过程如图 4-3 所示。

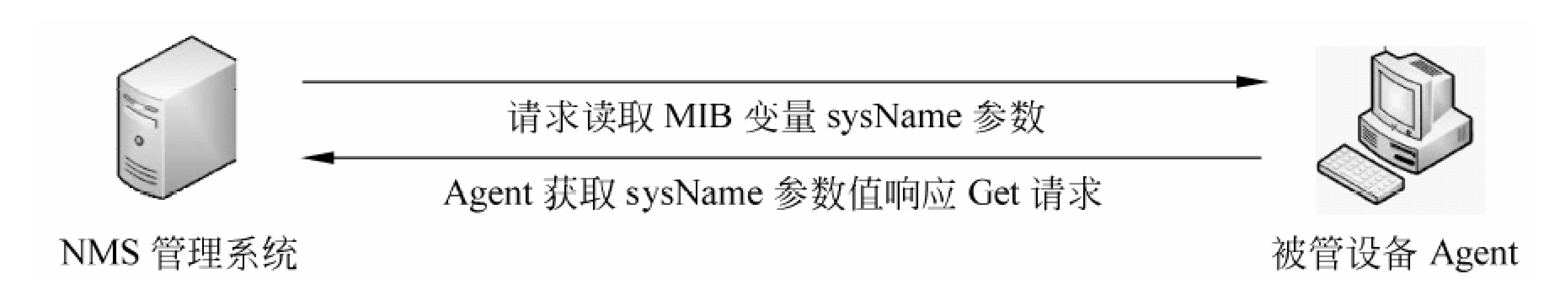


图 4-3　Get 操作

2. Set 操作

NMS 想要设置被管理设备 MIB 节点 sysName 为指定参数值（如 Device1），Agent 使用 private 为社区字符串，则操作过程如下：

NMS 给 Agent 发送 Set 请求，请求报文格式为 Version 字段（值为 2c），Community 字段（值为 private），PDU 设置对象（值为 sysName.0）设置参数值为 Device1。

Agent 收到请求，然后做出响应，如果 Set 操作成功，则响应 PDU 里设置参数值为设备的新名字（如 Device1）。如果设置失败，则在“错误状态”字段填写出错的原因。过程如图 4-4 所示。

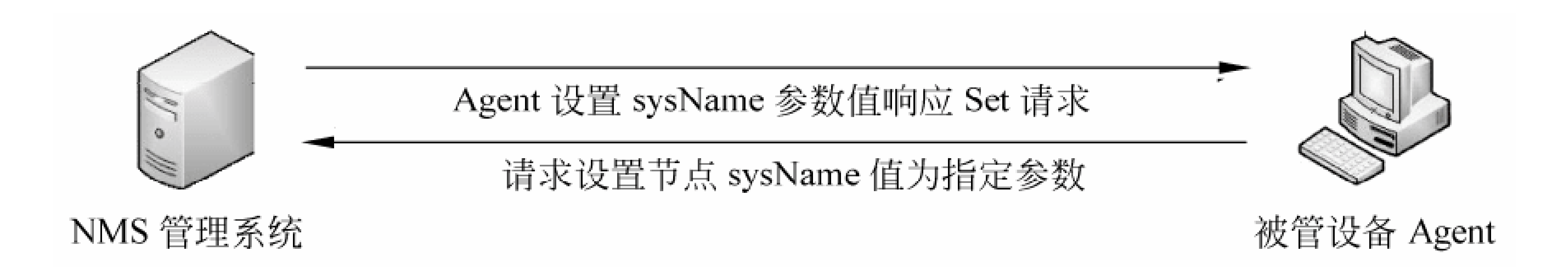


图 4-4　Set 操作

3. Trap 操作

当设备发生某些异常而需要通知 NMS 时，Agent 会主动发出 Trap 报文。例如，设备某端口网线被拔出，Agent 发送 linkDown 的 Trap 消息给 NMS。报文格式为 Version 字段（值为 2c），Community 字段（值为 public），PDU 包含了 OID 对象值及要报告的信息内容，过程如图 4-5 所示。



图 4-5　Trap 操作

SNMP 提供的 3 类操作，具体又可分为 7 种操作命令报文。在 SNMP v1 中包含 5 种类型的 PDU，有些是 Request（请求）报文，有些则是 Response（响应）报文。具体包括 Get-Request、Get-Next-Request、Set-Request、Get-Response、Trap 。SNMP v2 版本中，又增加了两种 PDU，Get-Bulk-Request 和 Inform-Request，共计 7 种。

前面 3 种报文及 SNMP v2 中增加的两种报文均是由管理进程向代理进程发出的，另外的 Get-Response 和 Trap 命令则是代理进程发给管理进程的。需要注意的是，管理进程是用端口 162 来接收响应报文和 Trap 报文的，而代理进程端则是用端口 161 接收 Get 和 Set 请求报文，如图 4-6 所示。

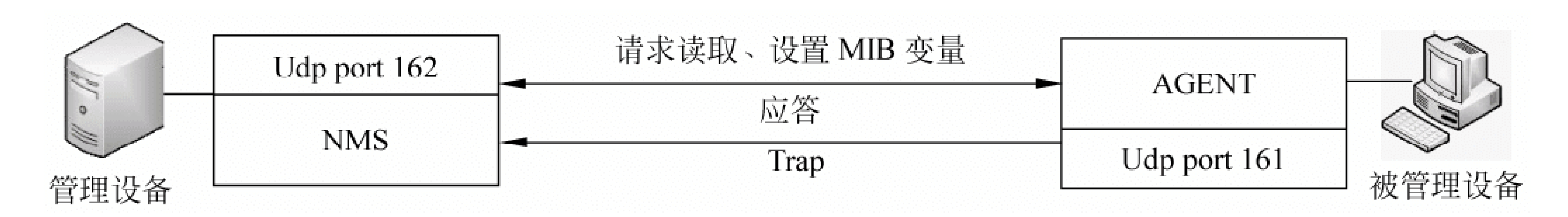


图 4-6　SNMP 协议数据包格式

在报文的数据包中使用数字代码来区分报文的种类。PDU 报文种类及解释见表 4.2。

表 4.2　7 种 PDU 报文类型及操作解释

数字代码	PDU 名称	操 作 解 释
0	Get-Request	SNMP 管理者通过端口从 SNMP 代理中获取一个或多个 MIB 参数值，而 SNMP 代理则用 Get-Response 消息响应
1	Get-Next-Request	SNMP 管理者从代理进程处提取紧跟当前参数值的下一个参数值
2	Set-Request	管理进程对网络设备进行远程配置（如设备名、属性、配置某一个设备属性有效/无效等），可更改一个或多个 MIB 参数值
3	Get-Response	返回的一个或多个参数值。这个操作是由代理进程发出的，它是前面 3 种操作的响应操作
4	Trap	代理进程主动向 SNMP 管理站发出报文通知所发生的特定事件或重要事件，如线路故障、连接中断和恢复、认证失败等消息。管理进程接收代理发来的 Trap 报文，并记录在一个数据库中。网络管理员可以通过专用的应用软件从管理站上查看每个代理提供的管理信息
5	Get-Bulk-Request	SNMP v2 中提供的可以检索大块数据的请求，代理进程会根据设定值返回尽可能多的应答信息
6	Inform-Request	一个管理进程根据其应用的要求发给另一个管理站进程，请求后者向某个应用提供管理信息

此处对其中的 Trap 报文和 Get-Response 报文进行介绍。

Trap 报文信息：代理进程发送给管理主机的 Trap 报文信息有两种，通用 Trap 和企业自定义的 Trap。通用 Trap 信息包括 coldStart、warmStart、linkDown、linkUp、authentication 五种，通过数字信息代表不同的内容。其他的 Trap 则为企业自定义的 Trap 报文。下面介绍通用 Trap 代码及其描述信息，见表 4.3。

表 4.3 通用 Trap 报文信息

数字代码	名　　称	描　　述
0	coldStart	代理进行了初始化
1	warmStart	代理进行了重新初始化
2	linkDown	一个接口从工作状态变为故障状态
3	linkUp	一个接口从故障状态变为工作状态
4	authentication Failure	从 SNMP 管理进程接收到具有一个无效共同体的报文

Get-Response 响应信息：管理进程向代理进程发送 Get 或 Set 报文，代理进程通过 get-response 将返回应答信息。其返回的信息通过 0～5 的数字代码分别代表不同的应答信息，这些应答信息被称为差错状态（Error Status），见表 4.4。

表 4.4 差错状态描述

数字代码	名　　称	描　　述
0	NoError	一切正常
1	TooBig	代理无法将回答装入到一个 SNMP 报文之中
2	NoSuchName	操作指明了一个不存在的变量
3	BadValue	一个 Set 操作指明了一个无效值或无效语法
4	ReadOnly	管理进程试图修改一个只读变量
5	GenErr	某些其他的差错

4.2.5 SNMP 安全性简介

SNMP Agent 功能非常强大，它们提供了对设备重要部分的访问和配置，但同时也对网络管理产生了极大的安全隐患。例如，代理程序提供了对 MIB 读写的功能，而大多网络代理中都默认使用 public 作为读认证字符串和 private 作为写认证字符串。如果社区字符串被通过数据包捕捉工具捕捉或者被猜测出，那么通过 SNMP Set 命令或者 MIB 浏览工具，能够很容易地更改网络接口配置参数，导致接口失效。所以更改默认的社区字符串对于网络安全是非常必要的。

目前，大多网络使用的仍是基于社区字符串的安全认证方式。而这种身份验证模型被认为是不安全、不可靠的。它存在的主要安全问题就是协议不提供加密功能，以及 SNMP 数据包在交换过程中携带了社区字符串信息。因为 SNMP 协议安全性的欠缺，大多数站点禁止管理代理设备的设置操作，但同样也限制了 SNMP 协议的应用。

要避免 SNMP 服务带来的安全风险，最彻底的办法是禁用 SNMP。如果不需要通过 SNMP 来管理网络，那就没有必要开启该服务的应用。下面介绍在常见的 Windows 和 Linux 系统中如何禁用 SNMP 服务。

1. Windows XP 和 Windows Server 2003 上禁用 SNMP 服务

在 Windows XP 和 Windows2K 系统中，在最初安装时，默认不安装 SNMP 服务，但许多软件会自动启动该服务的安装。如需要禁用 SNMP 服务，进入到【控制面板】，并选

择【服务】选项，从服务的清单中选择 SNMP 服务，然后通过快捷菜单打开其“属性”对话框，将启动类型改为“禁用”即可。

2. Cisco 和 H3C 网络设备

在 Cisco 的网络设备中，执行 No SNMP-server 命令禁用 SNMP 服务。如果要检查 SNMP 是否关闭，可执行 Show SNMP 命令。在 H3C 网络设备中，使用命令 Undo snmp-agent 则关闭 SNMP 服务的代理。

3. Redhat Linux 中禁用 SNMP 服务

在 Redhat Linux 系统中，可以用 Linuxconf 工具从自动启动的服务清单中删除 SNMP，或者直接从/etc/services 文件中删除启动 SNMP 的行。

除了禁止 SNMP 服务的运行，采用其他方式也能够加强 SNMP 协议的安全性，例如使用 IP Sec（IP 安全协议）、创建 IP 安全策略、配置防火墙策略等。由于本书主要介绍 SNMP 协议的应用，所以对安全性不做更多的讲解。

4.2.6 管理信息结构 SMI 介绍

SMI（管理信息结构）是简单网络管理协议体系中的一部分，用于定义管理信息库 MIB 的结构、MIB 中使用的数据类型及具体数据对象的编码方式等。SMI 规定了 MIB 的数据对象管理采用树状层次结构，结构树的分支表示的是数据对象的逻辑分组，树叶代表各个数据对象（也叫节点 Node），每个节点对象都有一个特定的名称标识，这个名称被称为对象标识符（Object Identifier），对象标识符是由一组统一格式的数字组成。

SNMP 协议通过遍历 MIB 树型目录中的叶子节点来访问 MIB 中的数据变量。SNMP 在访问数据对象的过程中，从树根开始查找树叶节点，每经过一个分支就记录该分支的数字序号，最终找到要访问的数据对象所记录的数字序号就成为该节点对象的名称。所以对象标识符唯一标识了节点的同时也体现了数据对象在 MIB 树结构中的位置。

同时，SMI 还规定了数据对象的数据类型，例如 Interger、UInteger32（无符号 32 位整数）、Octet String（任意二进制或文本数据，通常长度限制在 255 个字符内）、IpAddress（IP 地址）、Counter32（表示一个非负的整数，可递增到 32 位最大值－1 ）、Counter64（与 Counter32 相同，最大值为 64 位的最大值－1）。

4.2.7 管理信息数据库（MIB）介绍

大多数网络中，都或多或少采用了多个制造商的设备。为了使管理站能够与所有这些不同设备进行通信，SNMP 协议详细地规定了每种代理应该维护的确切信息以及提供信息的标准格式，并将这些对象信息都存放在 MIB 中。

MIB（管理信息数据库）包含了被管网络设备中各种类型数据对象的信息存储库，如设备的名称、硬件信息、运行时间、接口速度等。网络管理系统可以通过网络管理代理软

件来控制这些 MIB 数据对象，实现对网络中设备的信息读取、状态控制、配置或监控。现在已经定义的有几种通用的标准 MIB，这些数据库中包括了必须在网络设备中支持的特殊对象。目前使用最广泛、最通用的是第 2 版，即 MIB-II。

在 RFC1213 说明文档中详细定义了 MIB-II 的对象和标准，包括详细定义了 MIB 包含的 11 个功能组，共 171 个对象。

4.2.8 MIB 结构

MIB 的公共管理结构采用的是树形结构，如图 4-7 所示。MIB 对树结构中数据对象节点采用统一格式的标识符来进行命名，例如，{1.3.6.1.2.1}{1.3.6.1.4.1}。这些数据对象的参数值可以被 SNMP 管理者通过 Get 或 Set 操作进行读取和修改，设备中的 SNMP 代理则对管理者的 Get 和 Set 请求进行应答。

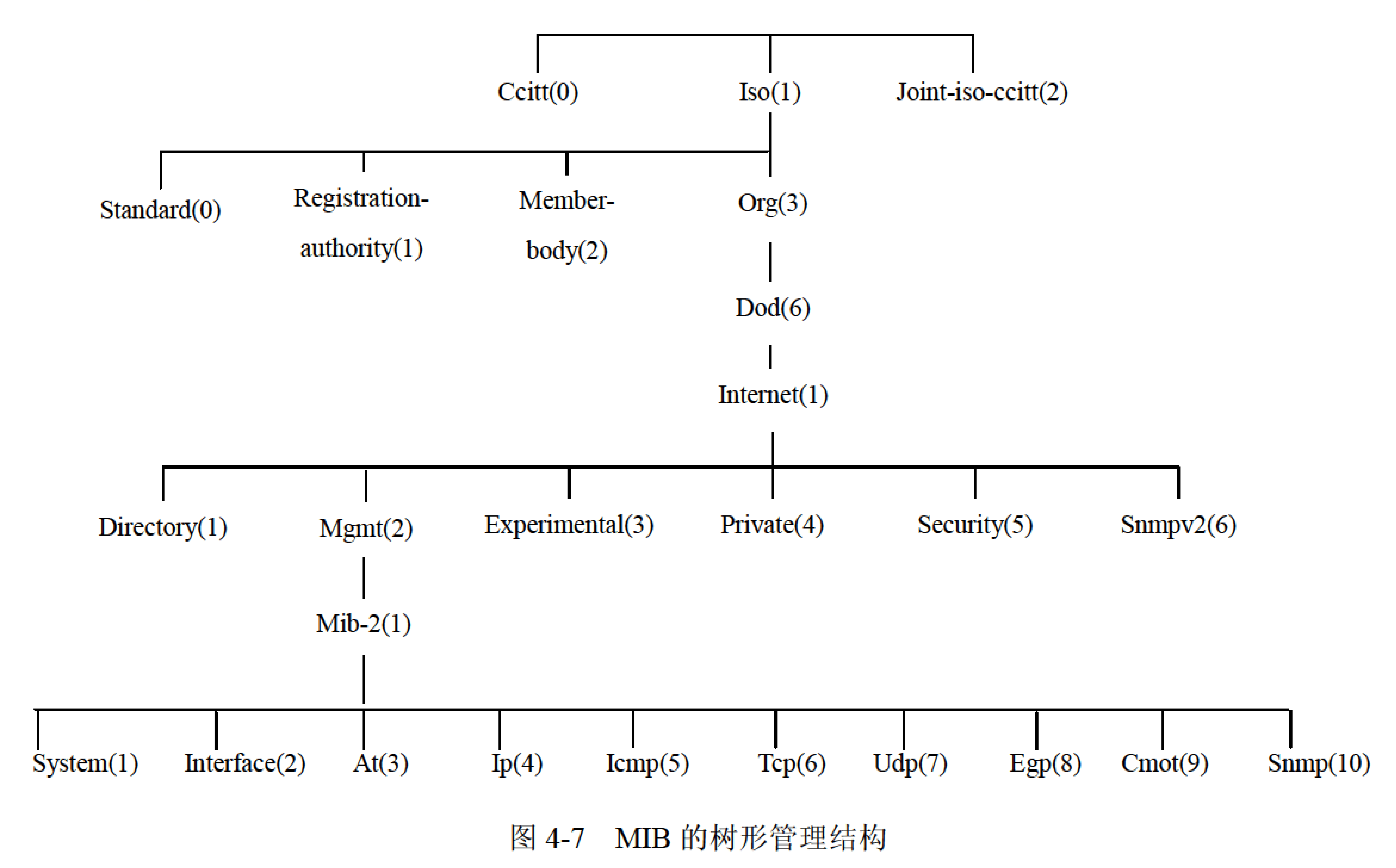


图 4-7　MIB 的树形管理结构

MIB 结构树包含 3 个顶级对象，即 ISO、ITU-T 和这两个组织的联合体 Joint-iso-ccitt。在顶级对象 ISO 的下面是定义 MIB 的组织 Org（标识为 3）。组织下方是由美国国防部（Department of Defense）定义的子树结构（标识为 6）。再下面就是当时由 Dod 管理的 Internet（标识为 1）节点。如果需要标识 Internet 中的某个对象，按照定义取该对象的访问路径作为标识，则对象标注为 iso.org.dod.internet，使用简化数字则标识为{1.3.6.1}。继续往下遍历节点，那么位于 Mib-2 分支下的节点被标识为{1.3.6.1.2.1}。

实例：在 system 子树中包含 sysDescr（系统描述）的节点，其完整标识应该是 iso.org.dod.internet.mgmt.mib-2.system.sysDescr，简化的数字标识则为 1.3.6.1.2.1.1.1。

注意：standard（0）：其下属节点指定给各个国际通用标准。

registration-authority（1）：该节点保留给新成立的 OSI 注册机构。

member-body（2）：其下属节点指定给 ISO/IEC 的成员组织，每个下属节点代表一个国家。

identified-organization（3）：其下属节点指定给可以通过国际组织确认的节点。目前有两个已确认的组织，即 NIST 和 Dod。

4.2.9 重要的 MIB 节点对象

下面介绍一下在网络管理中最常用也是最重要的对象组，即 MIB-II（1）。MIB-II 是 SNMP 协议中的基础 MIB，几乎所有支持 SNMP 的设备都支持 MIB-II。它实现了设备的通用管理。MIB-II 描述为 iso.org.dod.internet.mgmt.mib-2（1.3.6.1.2.1）。

在最初的 MIB-I 版本中，定义了 8 个对象组，分别用 1～8 进行标号。而 MIB-Ⅱ版本在 MIB-I 的基础上做了扩展，增加了 SNMP 和 CMOT 两项，标号为 8、9。随着 MIB 数据对象的不断壮大，其包含的对象组也不断增加，目前已经超过 40 个。其最重要的 10 个对象组说明见表 4.5。

表 4.5 MIB-II 管理的数据对象组

序号	类　　别	标号	所包含的数据对象信息
1	System	（1）	系统组：硬件、操作系统和网络软件的名称和版本等完整信息
2	Interfaces	（2）	接口组：网络接口硬件、版本及接口状态等信息
3	Address Translation	（3）	地址转换组：地址转换（例如 ARP 映射）信息
4	Ip	（4）	协议组：Internet 软件（IP 分组统计）
5	Icmp	（5）	Internet 控制报文协议组：ICMP 信息及统计
6	Tcp	（6）	传输控制协议组：TCP 参数和统计
7	Udp	（7）	用户数据报文组：UDP 协议及通信量统计
8	Egp	（8）	外部网关协议组：EGP 协议信息及其通信量统计
9	CMOT	（9）	传输组：公共管理信息与服务协议数据对象（已废止不用）
10	SNMP	（10）	SNMP 协议组：简单网络管理协议相关数据对象

除此之外，树结构中比较重要的对象或对象类如下：

- iso.org.dod.internet（1.3.6.1）：包含 TCP/IP 协议相关的 MIB 部分。
- iso.org.dod.internet.mgmtmgmt（1.3.6.1.2）：包含系统/网络界面/各种应用程序/网络协议/路由协议的基本监控功能。
- iso.org.dod.internet.private（1.3.6.1.4）：企业私有的 MIB 库，描述了企业私有的设备特性。

在本书最后的附录 A 中，详细介绍了 10 个对象组及其节点对象的作用。

4.2.10 MIB 管理工具 MIB Browser 的使用

MIB Browser 工具集成了访问 SNMP 设备的命令，可遍历 MIB 结构树获取对象信息，

并以图形的形式来表示各个分支和树叶对象。

该工具有众多不同开发商提供的免费程序供下载，例如 MG-SOFT MIB Browser 、HiliSoft MIB Browser、KS-Soft MIB Browser 等。这些工具都能够用于连接各类设备以获取 MIB 信息。在功能完备的 MG-SOFT 和 HiliSoft MIB Browser 中，提供了相对较多的命令支持，如 SNMP Get、SNMP GetNext、SNMP GetBulk、SNMP Set 命令及捕捉 Trap 信息等。而在 KS-Soft MIB Browser 中，仅支持最常用的 SNMP Get 和 Get Next 命令，使用较为简单，但同样能够获得完备的 MIB 树结构信息。

此处旨在通过 MIB 浏览工具对 MIB 的结构、参数对象和命令方式进行了解和熟悉。以下以 KS-Soft MIB Browser 工具为例介绍如何获取 MIB 对象信息。

在 KS-Soft MIB Browser 主界面中，展现了整个 MIB 树结构，可点击树的分支展开各节点。在界面下方显示了所选节点的附加信息，包括 MIB（节点路径）、OID（对象标识）、SYNTAX（数据类型）、Access（访问方式）、Status（状态）和 Description（描述信息），如图 4-8 所示。

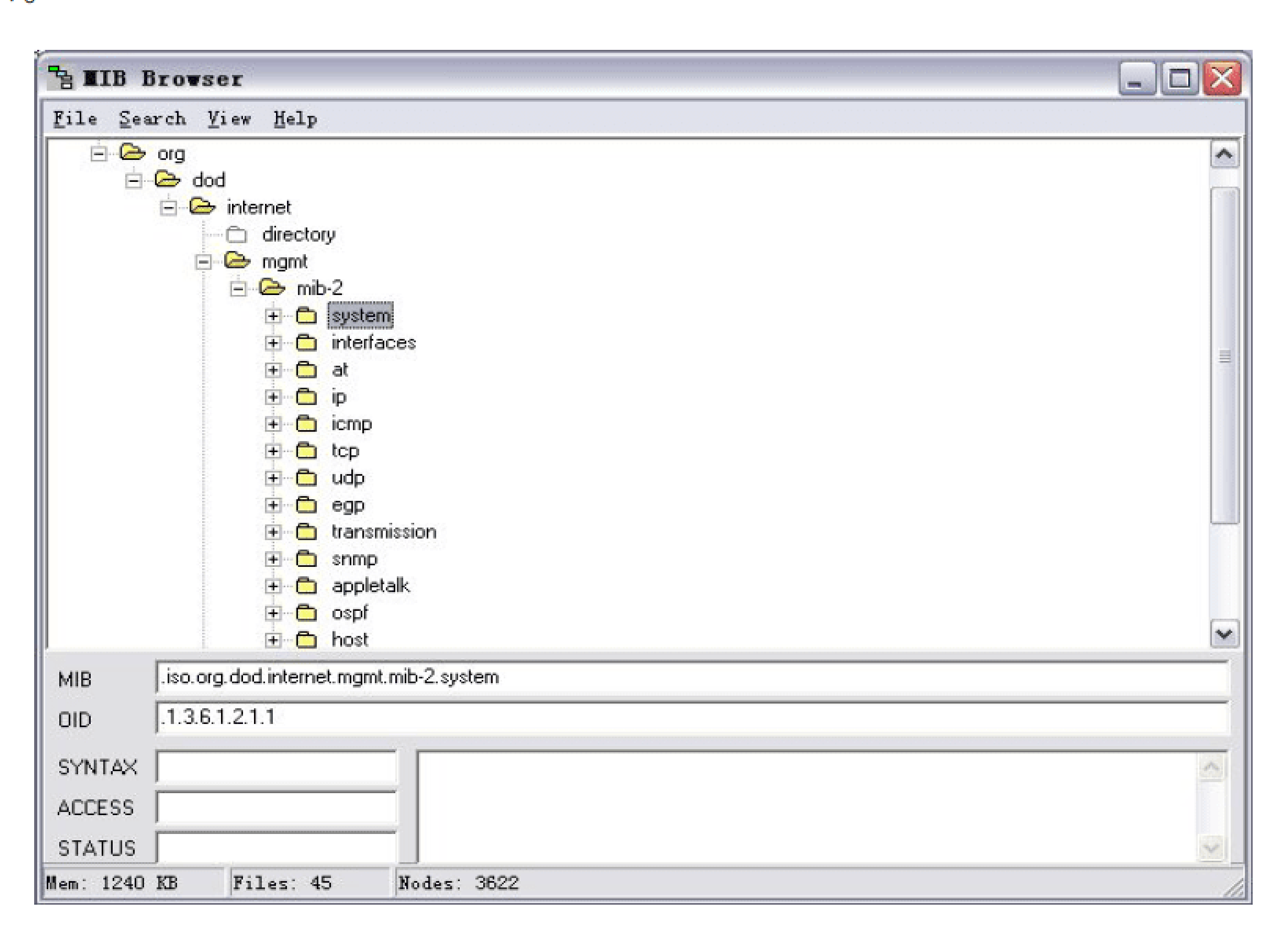


图 4-8 MIB Browser 程序主界面

如果需要获取指定 MIB 节点的信息，在界面树状图中选择指定节点，然后打开 View 菜单，选择 Get counter value 菜单命令，即可打开 SNMP Get 对话框进行获取对象信息的操作（或在所选节点上，打开快捷菜单并选择 Get Value 菜单命令）。例如，选择 system 对象中的 sysDescr 节点，打开 Get value 对话框，如图 4-9 所示。

在如图 4-9 所示界面的 Agent（add）文本框中，输入本地或者远程服务器的 IP 地址，在 Community 文本框中输入要访问 IP 设备的社区字符串，然后单击 Get 按钮，将获得对象的 OID 值及其参数。如果输入了错误的社区字符串，或者不能 Ping 通远程服务器，或者对端服务器未开启 SNMP 服务，那么将提示无法连接到远程 SNMP 代理，如图 4-10 所示。

在 MIB Browser 中可加载标准的 MIB 文件和私有的 MIB 文件。很多私有设备的 MIB

文件并不包含在 MIB 库中，需要另外加载到 SNMP 访问工具中。只要设备的 SNMP 代理支持加载的 MIB 文件，SNMP 就能够获取该设备特定的 MIB 信息。例如，需要访问 Windows Exchange 服务更多的 MIB 信息，首先需要下载定义了 Exchange 服务对象的 MIB 文件，然后通过 MIB Browser 程序将 MIB 加载到设备中。步骤如下：

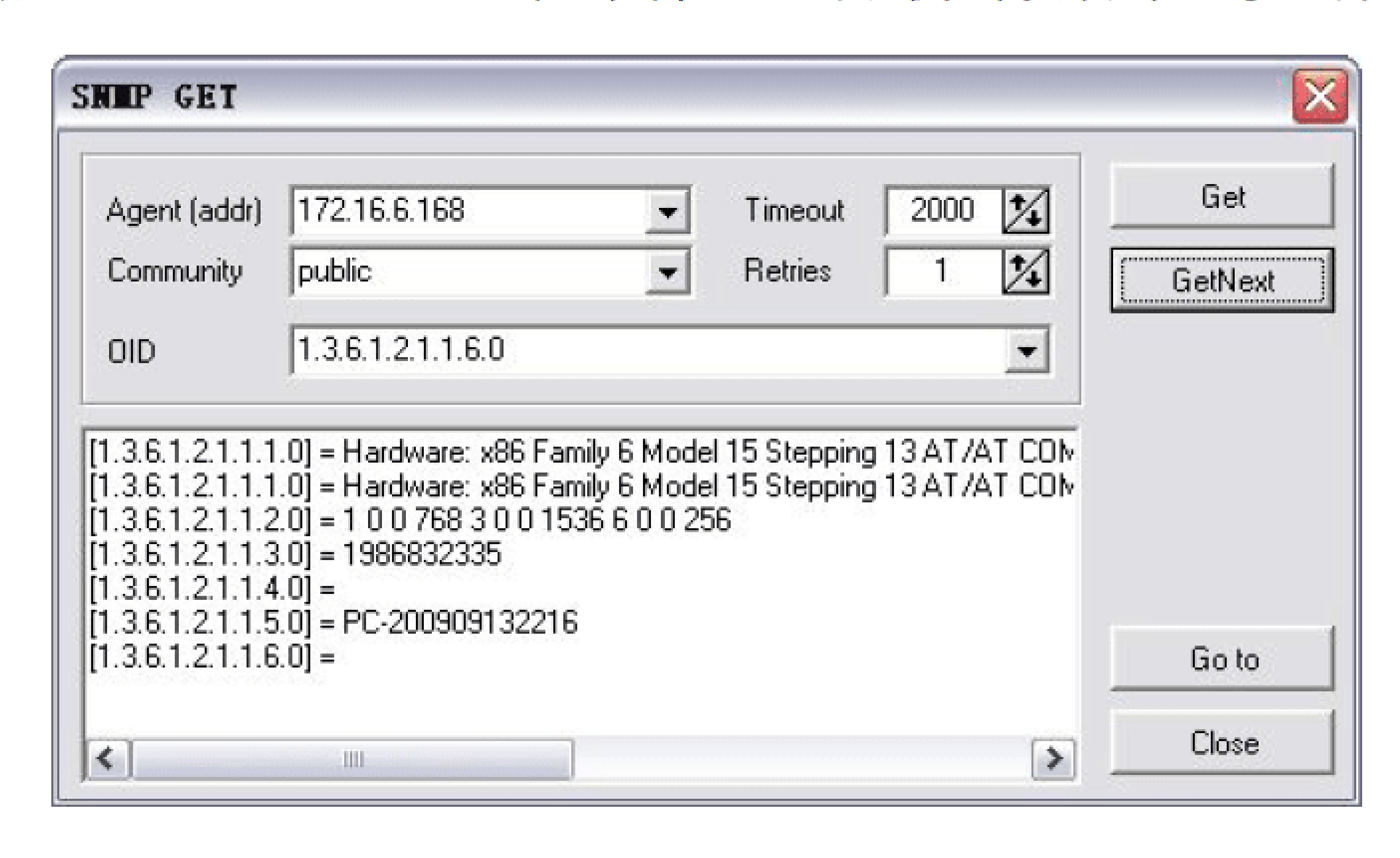


图 4-9　打开 SNMP GET 界面



图 4-10　无法连接远程 SNMP 代理提示

（1）在程序主界面打开 File 菜单，选择 Append MIB File 菜单命令，将显示【打开】对话框（如图 4-11 所示），选择需要加载的 MIB 文件后 MIB Browser 会编译并加载文件。

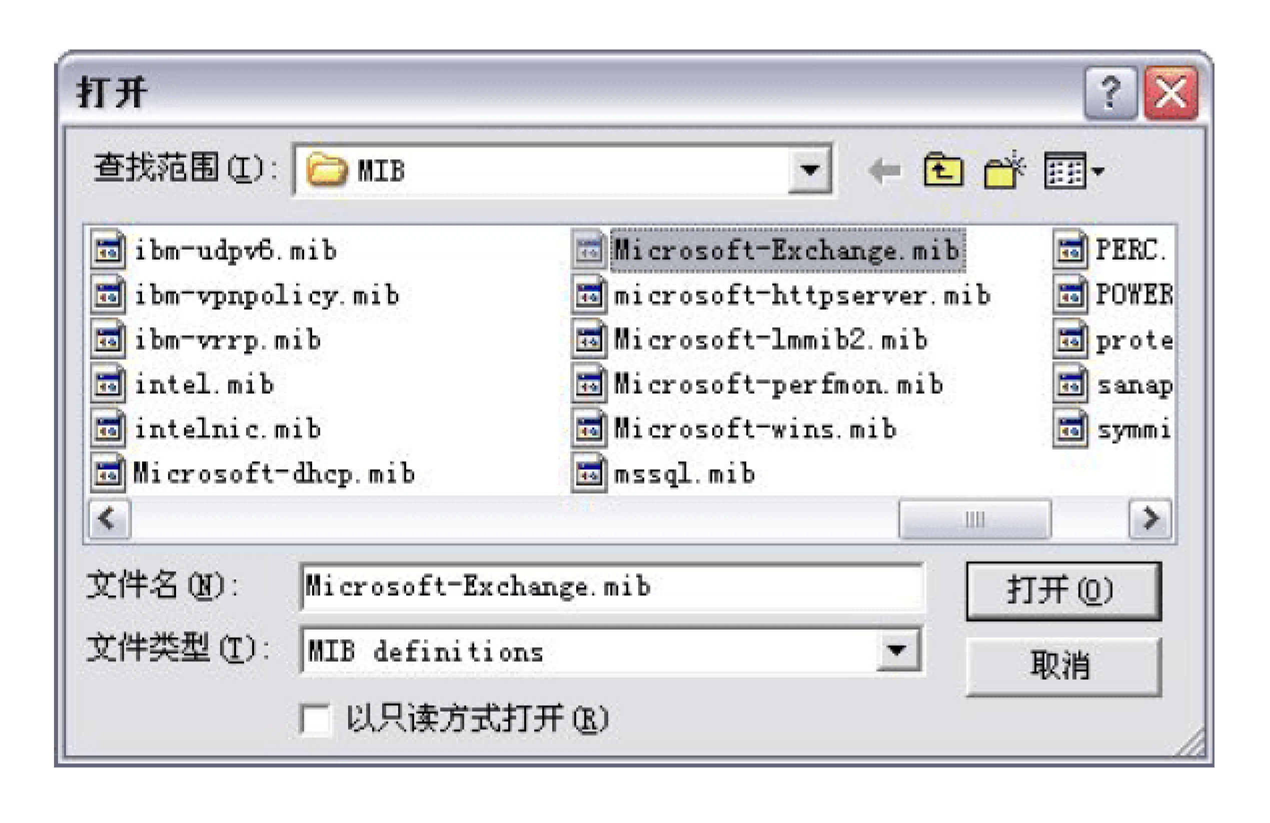


图 4-11　加载定义 Exchange 服务的 MIB 文件

（2）如果文件信息完整，MIB Browser 对文件进行编译通过后，可看到所加载 MIB 文件的数量，如图 4-12 所示。

（3）完成加载操作后，在主界面中可查看加载的 MIB 文件。选择 View | Statistics 命令，可看到加载文件的数量和时间等信息，如图 4-13 所示。

（4）加载完成后的文件将存储到 MIB 数据库中，如果需要备份 MIB 库，可选择 File | Save database 命令备份当前的数据库文件。选择 Load database 命令，则能够还原备份数据库文件，以替换当前库文件。

注意：如果需要通过网管监控程序去读取特定的 MIB 对象信息，则需要将 MIB 文件加载到网络监控程序中。当然，前提是网管程序支持 MIB 文件的加载。

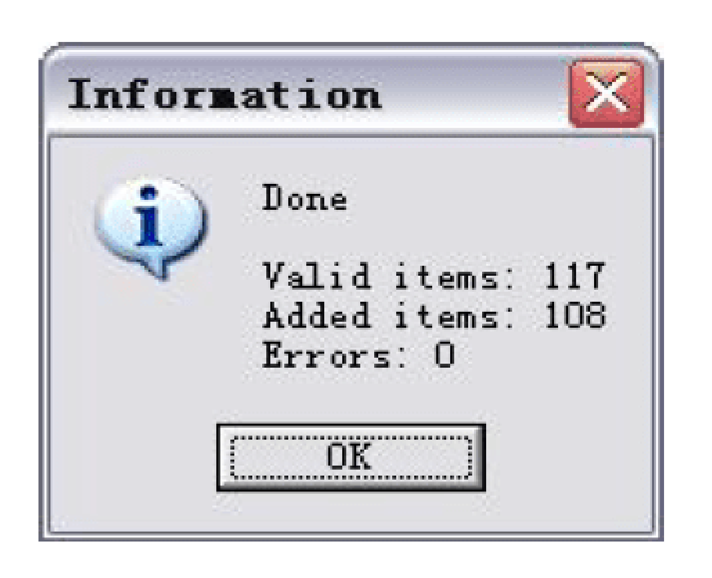


图 4-12　提示编译和加载 MIB 文件成功

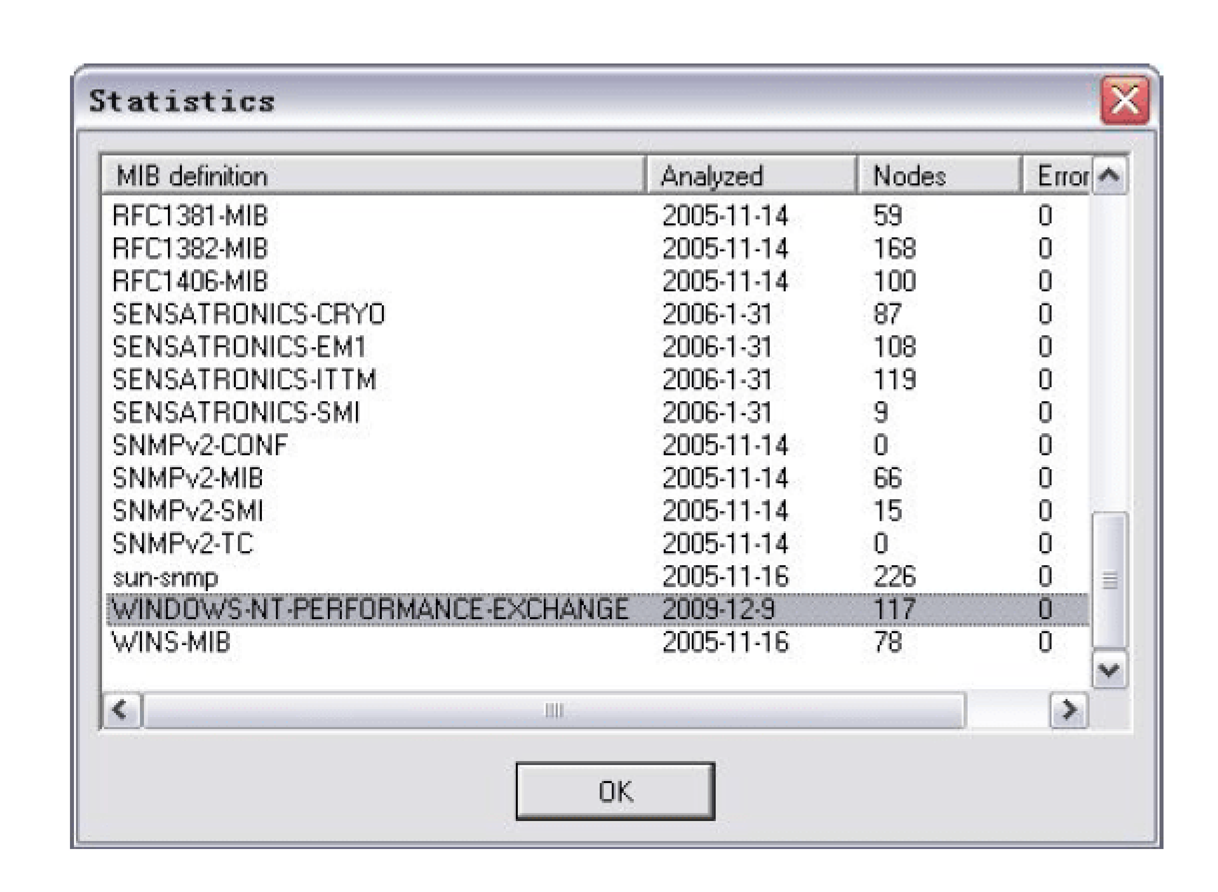


图 4-13　查看加载的 MIB 文件

4.3　SNMP 服务的配置和应用

为了从网络设备中通过 SNMP 协议采集信息和监测状态，在网络设备中需要开启 SNMP 代理服务(SNMP Agent)。在 Windows 和 Linux 系统主机中，默认未安装 SNMP Agent 服务，需要进行代理程序的安装。SNMP 代理能够响应 SNMP 协议的询问和发送 Trap 信息至网管程序。

下面介绍在 Windows 主机中添加 SNMP 代理服务。

4.3.1　在 Windows 服务器上安装 SNMP Agent

在 Windows Server 2000\2003 及 Windows XP 系统中均采用同样的方式添加 SNMP 服务。打开 Windows 系统控制面板中的【添加或删除程序】，选择【添加/删除 Windows 组件】，在添加组件对话框中选择【管理和监视工具】并双击该选项打开对话框，在弹出的对话框中选择两个子选项（WMI SNMP 提供程序和简单网络管理协议），最后单击【确定】按钮，即可安装 SNMP 组件，如图 4-14 所示。



图 4-14　添加 Windows SNMP 组件

4.3.2 在 Windows 服务器上配置 SNMP Agent

当 SNMP 管理站向设备 SNMP Agent 发送查询命令时，会将管理站提供的社区字符串与代理的字符串进行比较。必须匹配通过才能获得访问对端设备的权限。所以在为设备安装 SNMP 组件后，需要对 SNMP 服务做简单的配置。主要是配置在通过 SNMP 获取信息时的身份验证字符串，即社区字符串 Community String。下面介绍如何配置 Windows 系统中的 SNMP 服务，步骤如下。

（1）在 Windows 控制面板中，打开【管理工具】，选择【服务】选项，在系统服务列表中找到 SNMP 服务【SNMP Service】，并双击打开其属性界面（如图 4-15 所示），在【常规】选项卡中可以更改 SNMP 服务启动的方式。

（2）在【登录】选项卡中，选择在系统账户下或某指定用户下使用 SNMP 进程。默认选择【本地系统账户】，即能够登录本机账户，均能使用 SNMP 进程，如图 4-16 所示。

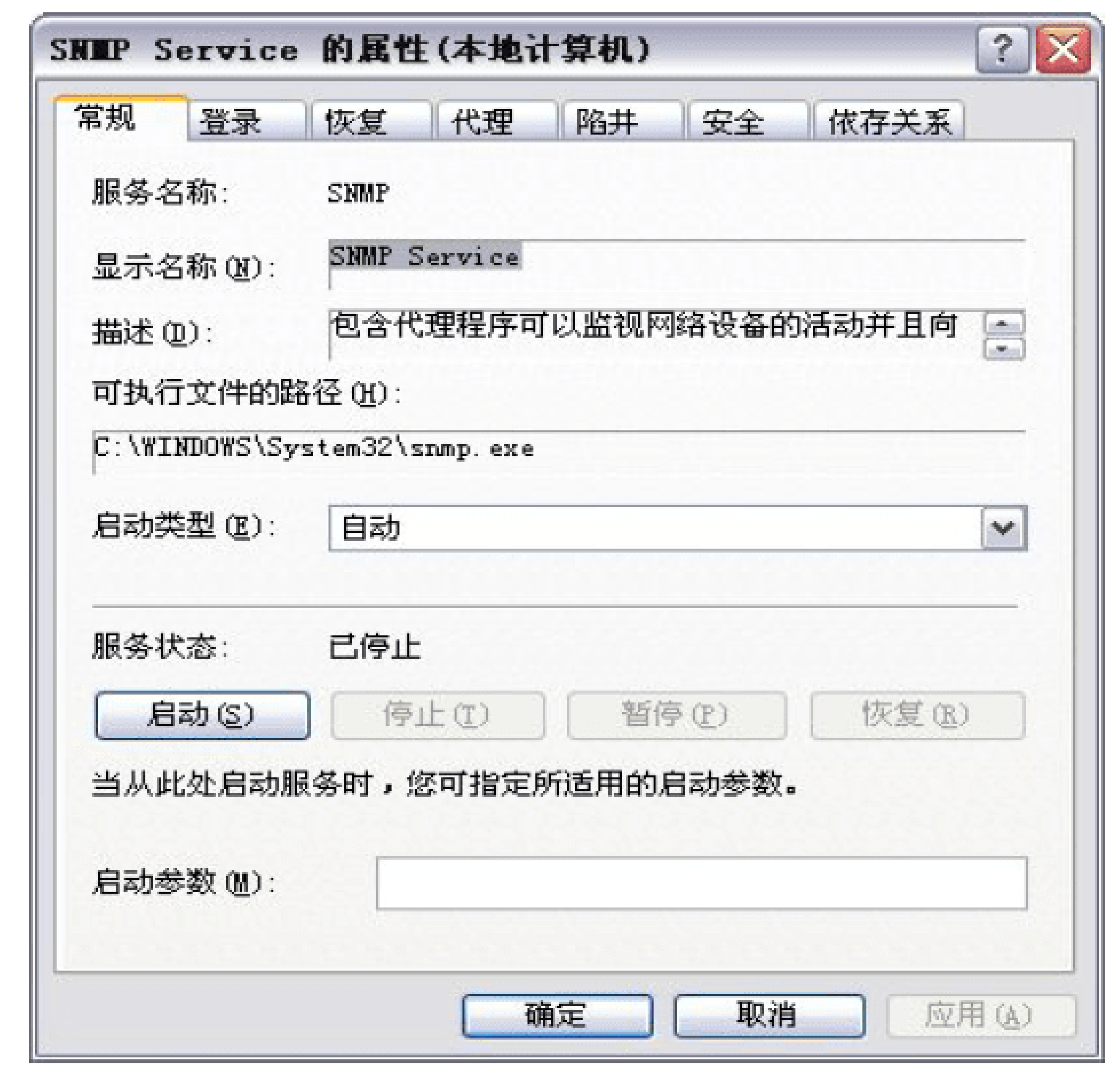


图 4-15 配置 SNMP 常规选项

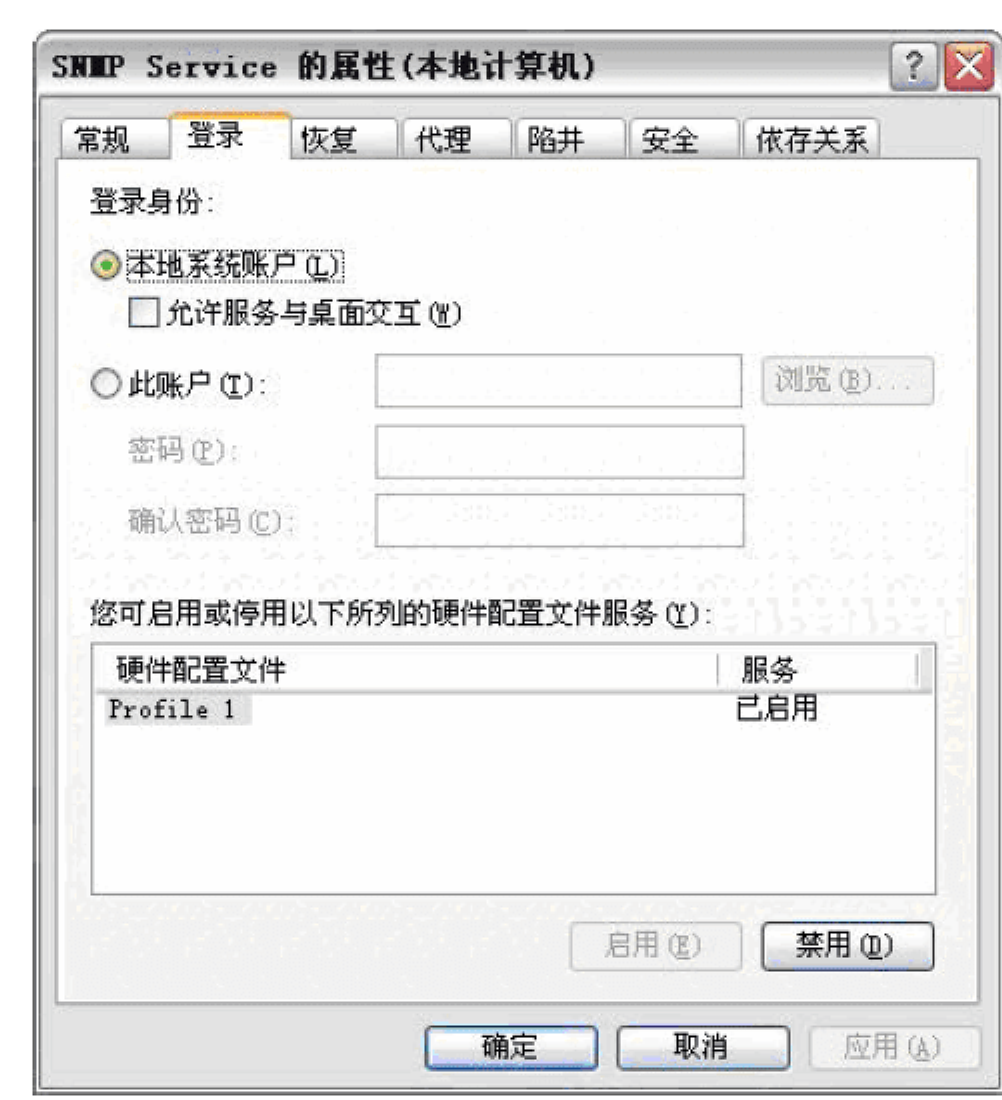


图 4-16 配置 SNMP 登录选项

（3）在【恢复】选项卡中，可选择当服务失败时计算机所做的反应，可选择在进程第一次失败时重启服务等。在【代理】选项卡中可输入联系人信息和位置信息，例如物理地址，楼层信息等，如图 4-17 所示。在恢复和代理配置中，不需要做更多的配置，保持默认配置即可。

- 服务：Windows 要代理的服务。
- 物理：指定计算机是否管理物理设备，如硬盘分区。
- 应用程序：指定计算机是否使用任何通过 TCP/IP 发送数据的程序。
- 数据链接和子网：指定此计算机是否管理 TCP/IP 子网或数据链接。
- Internet：指定此计算机是否充当网关（路由器）。
- 端对端：指定此计算机是否充当 IP 主机。

（4）在【陷井】选项卡中，如果该 SNMP 主机发生了任何特定事件，SNMP 服务都会生成陷井消息并将消息发送至陷井目标。陷井目标必须是正在运行 SNMP 管理软件的已启用网络的主机，可由计算机名、IP 或 IPX 地址表示，如图 4-18 所示。



图 4-17　配置 SNMP 代理选项

SNMP Service 的属性(本地计算机)
常规 登录 恢复 代理 陷井 安全 依存关系
SNMP 服务通过 TCP/IP 和 IPX/SPX 通讯协议提供网络管理。如果需要陷阱，必须指定一个或更多的团体名称。陷阱目标可以是主机名、IP 地址或 IPX 地址。
团体名称(C)
trap
添加到列表(L)
从列表中删除(R)
陷井目标(T):
172.16.6.1
添加(D)...
编辑(E)...
删除(M)
确定 取消 应用(A)

图 4-18　配置 SNMP 陷井选项

（5）在【安全】选项卡中（如图 4-19 所示），如果想在身份验证失败的时候触发陷井信息，则需要选择【发送身份验证陷井】复选框。在该界面中，还需要为 SNMP 服务至少配置一个默认的团体名称，也就是社区字符串。public 作为公认的只读字符串被普遍使用，当然从安全角度考虑，最好更改或删除默认的社区字符串，而使用自定义字符串作为访问的认证。



图 4-19　配置 SNMP 安全选项

设备在被访问时，如果 SNMP Agent 收到的请求字符串并未在该列表中，则 SNMP Agent 会触发一个认证失败的 Trap。如果该列表未定义任何社区字符串，则 SNMP Agent 将拒绝任何的 SNMP 请求。

此处，在【接受团体名称】中，添加默认的 publlic 作为读取设备信息默认的认证字符串，添加 private 作为具备更改设备 SNMP 配置信息权限的认证字符串。如果允许接收来自网络上任何主机的 SNMP 请求，则需选择【接受来自任何主机 SNMP 数据包】复选框，要想限制接收 SNMP 数据包，需要选择【接受来自这些主机的 SNMP 数据包】复选框，并添加允许接受 SNMP 请求的主机名、IP 或 IPX 地址。

注意：社区名称区分大小写，即 public 和 Pubilc 是两个不同的社区字符串。

（6）设置完成后，需要在 Windows 系统下测试 SNMP 服务是否能够正常获取 MIB 信息，可使用命令工具 Snmputil.exe。只需要下载该免费工具并复制到硬盘中（此处到 C 盘根目录），然后打开命令提示符界面，进入 Snmputil 所在目录，然后执行该工具即可。命令语法如下。

- 获取 MIB 信息命令：snmputil [get | getnext | walk] agent community oid
- 监听 Trap 信息命令：snmputil trap

其中，Get 为获取一个 MIB 对象信息，Getnext 为获取下一个对象信息，Walk 为获取批量信息，agent 表示代理进程的 IP 地址，community 表示社区字符串，oid 表示 MIB 对象 ID。

例如，获取本机系统信息（Oid 值为.1.3.6.1.2.1.1），如果顺利取得 MIB 对象信息，则 SNMP 服务运行正常。命令获取对象值后如图 4-20 所示。

Snmputil 还可监听 Trap 信息，用于捕捉陷井信息。它可以接收远程主机主动发来的 Trap 信息。例如，在网管服务器命令行提示符界面中输入 snmputil trap 后回车，将启用对本地端口的 Trap 消息监听，如图 4-21 所示。然后将远程主机中的 Trap 消息目标设置为网管服务器，之后拔断远程主机的网线，远程主机将生成一个 linkdown 的 Trap 信息并发送至网管服务器，此时 Snmputil 监听程序将收到该 Trap 消息。

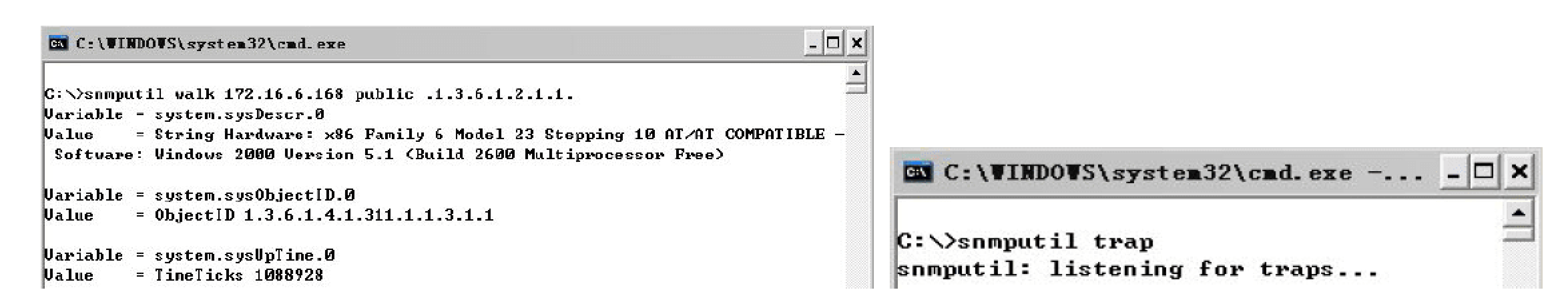


图 4-20 Windows 测试 SNMP 服务是否正常运行　　　图 4-21 SNMP Trap 监听服务

4.3.3 在 Windows 系统中使用第三方 SNMP 代理

在 Windows 操作系统中自带了 SNMP 组件，但如果该服务无法正常启动，或者其功能无法满足开发的需求，就需要采用第三方的 SNMP 代理工具。此处推荐使用最为广泛的 Net-SNMP，通过其官方网站 www.net-snmp.com 进行免费下载。网站中提供了支持

Windows 和 Linux 的各种版本安装包。

Net-SNMP 是一个免费的、开放源码的 SNMP 实现程序，以前称为 UCD-SNMP。它包括代理、SNMP 库、查询和设置 SNMP 代理消息、产生和处理 SNMP 陷井消息和多个管理工具的源代码。支持多种扩展方式，被广泛运用到 SNMP 程序和开发中。Net-SNMP 中提供了支持 SNMP 开发的 C 函数库，可供开发者开发 SNMP 应用程序。

1．在 Windows 系统中安装 Net-SNMP

下面介绍在 Windows 操作系统中安装和使用 Net-SNMP 的步骤。

（1）从互联网下载支持 Windows 操作系统的 Net-SNMP 免费安装包，名称为 Net-SNMP-5.4.2.1-1.win32.exe，并双击该安装包进行安装，如图 4-22 所示。

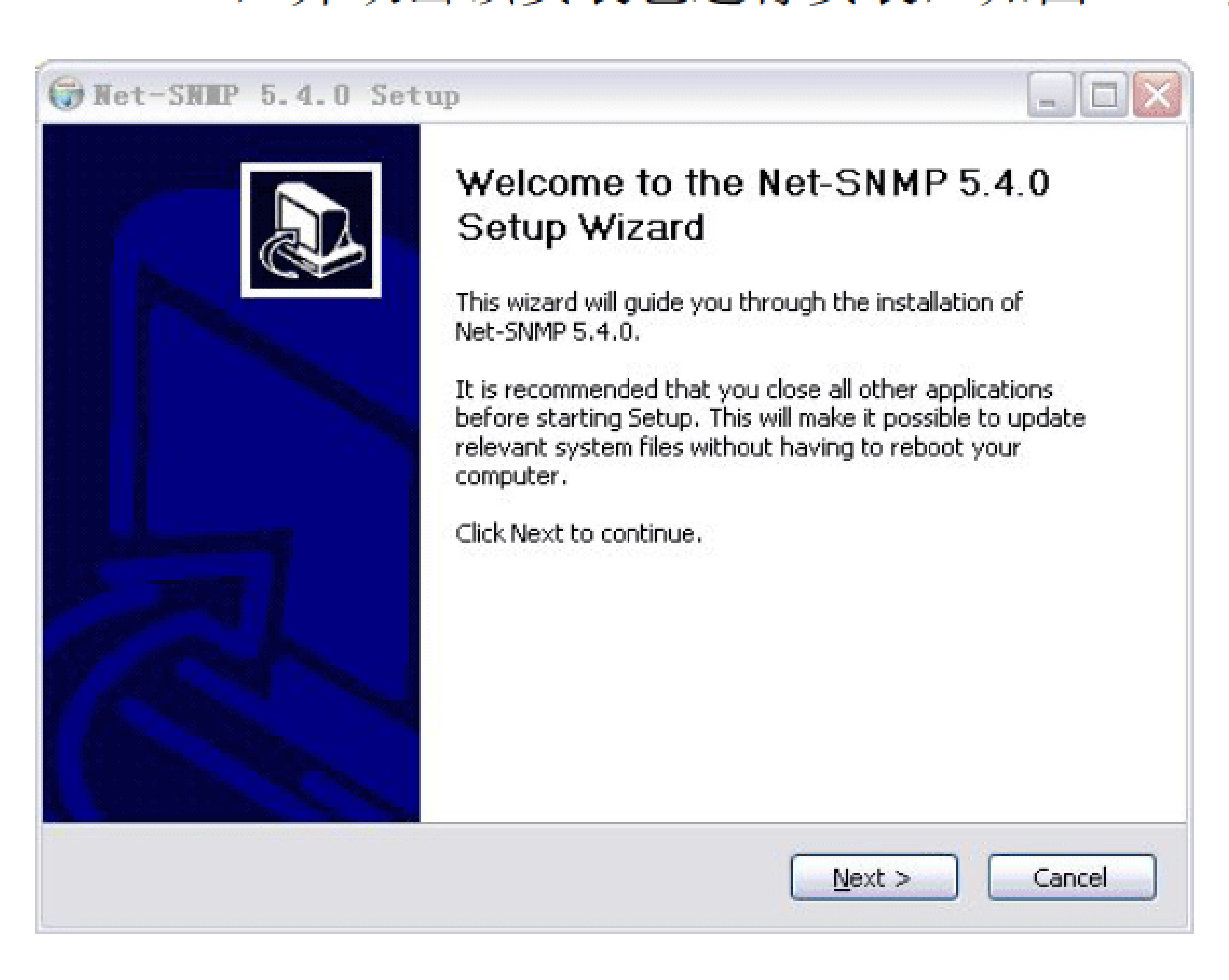


图 4-22 安装 Net-SNMP 程序

（2）选择下一步进入组件选择界面，选择基础组件、SNMP 代理和 Trap 服务组件。其中 SNMP 代理选择第二项 With Windows Extension Dll support 选项，以及 Perl 语言开发的支持组件 Perl SNMP Modules，本书不涉及程序开发，可以选择不安装，如图 4-23 所示。

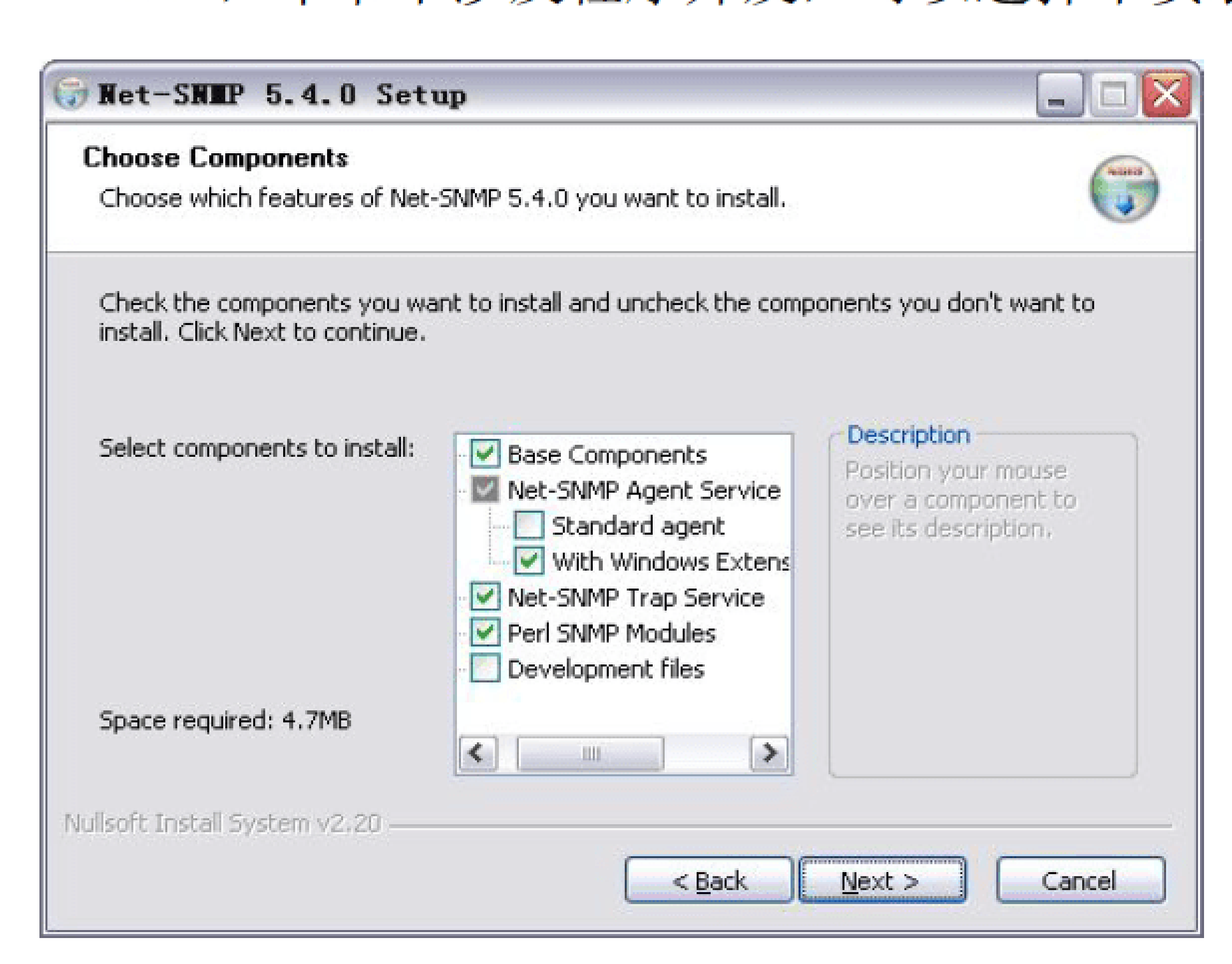


图 4-23 选择 Net-SNMP 的安装组件

（3）选择组件后进入下一步选择安装目录，此处选择默认的 c:\usr，则进入程序安装。在 Net-SNMP 安装完毕后，打开 Windows 开始菜单，将看到安装的 Net-SNMP 程序，如图 4-24 所示。

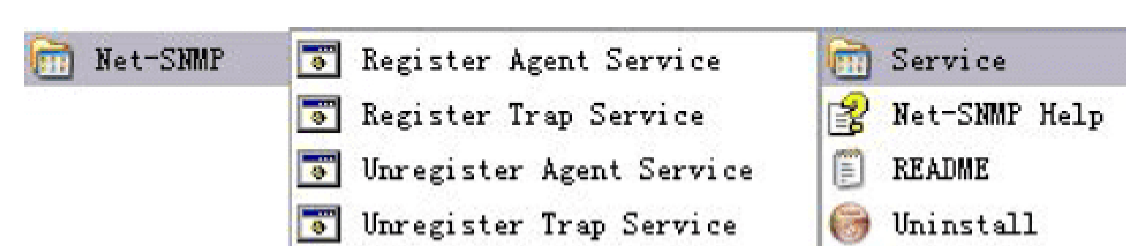


图 4-24　安装 Net-SNMP 完毕

（4）程序安装后，需要做简单配置才能正常启动服务。在安装目录 C:\usr\etc\snmp 下需要包含一个文件为 snmpd.conf 的配置文件，其内容可通过手工建立，也可将官方网站下载的该文件直接复制到目录中即可。此处选择直接下载 snmpd.conf 配置文件。在其官方网站 www.net-snmp.com 中下载文件名为 Net-snmp-5.4.2.1.zip 的压缩包，其中包含了所需的 snmpd.conf 文件。

将 snmpd.conf 文件复制至 C:\usr\etc\snmp 目录后，还需要在该文件中找到 com2sec local localhost public 行，并将该行中的 localhost 字符串更改为本机或需要访问本机的网管主机 IP 地址，如 com2sec local 172.16.6.168 public。

（5）在 c:\usr 目录下，单击 registeragent.bat 和 registertrapd.bat 这两个批处理文件，对代理和 Trap 服务进行注册，如图 4-25 所示。

（6）此时，Net-SNMP 服务已经加入 Windows 服务中。可以在【控制面板】|【服务】中看到 Net-SNMP 提供的两个服务，如图 4-26。





图 4-25　对 Net-SNMP 代理和 Trap 注册



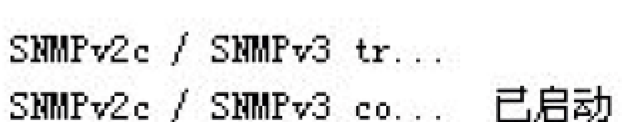




图 4-26　Net-SNMP 服务的启动

在图 4-26 中，可以看到该两项服务已经启动。除了在 Windows【服务】中启动或停止 Net-SNMP 外，还可以在命令提示符界面中启动和停止该服务，命令分别为 net stop "net-snmp agent" 和 net start "net-snmp agent"，如图 4-27 所示。

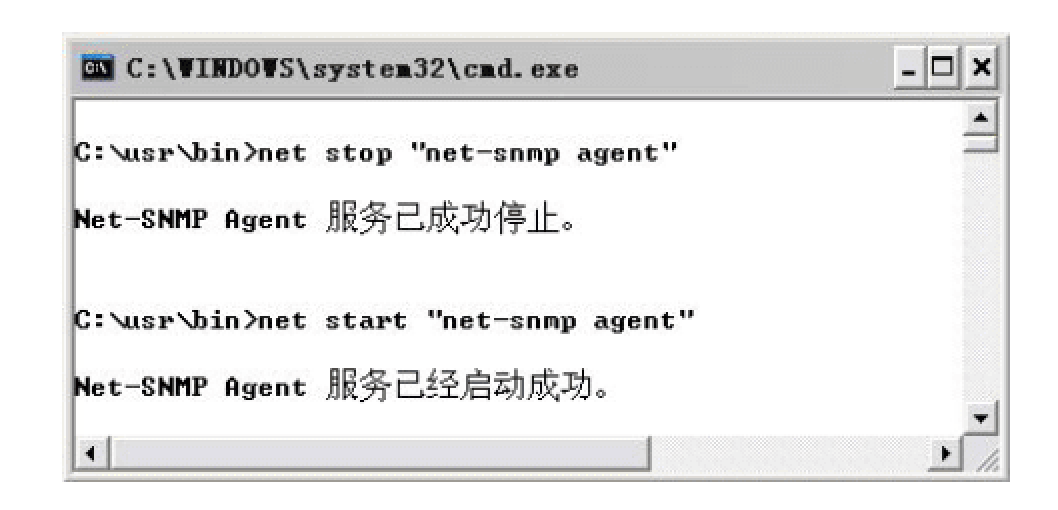


图 4-27　命令方式启动和停止 Net-SNMP

（7）安装配置完成后，需要对 Net-SNMP Agent 服务是否正常运行进行验证，其验证命令不同于验证 Windows 自带 SNMP 的 Snmputil 命令。在 Net-SNMP 中使用命令 snmpwalk 获取 MIB 信息，语法如下：

```
    snmpwalk （-v string version，string hostname，-c string community，string object_id [，int timeout [，int retries]]）
```

该命令为 SNMP 应用程序通过 SNMP GetNext 命令从网络实体中的 SNMP 代理获取 MIB 树节点信息，包括获取本机或远程主机，参数解释如下。

- -v string version：指定使用的 SNMP 版本，可输入-v 1/2c/3。
- string hostname：指定目标主机的主机名或 IP 地址。
- -c string community：访问目标主机的社区字符串（read community）。

- Object_id：目标对象 OID，此处可输入 OID 的完整标识或数字标识。如查看 MIB-II 下所有数据对象信息，可输入“iso.org.dod.internet.mgmt.mib-2”或简化路径 mib-2 或标识 1.3.6.1.2.1。如果该参数为空，则返回目标主机中所有 MIB 对象的信息。

例如，从本机（Ip=172.16.6.168，Community=public）中获取 MIB 对象参数值，可表述为以下 3 种方式，其返回的结果相同。

- snmpwalk -v 2c -c public 172.16.6.168 iso.org.dod.internet.mgmt.mib-2.system，查看 Mib-2 中的系统信息。
- snmpwalk -v 2c -c public 172.16.6.168 system，查看系统信息的简单标识描述。
- snmpwalk -v 2c -c public 172.16.6.168 1.3.6.1.2.1.1，查看系统信息的数字标识描述。

使用方式 2 来测试服务的启动，如果返回 MIB 信息，则表示 SNMP 服务启动正常。进入工具所在的目录 C:\user\bin，执行 snmpwalk 命令，结果如图 4-28 所示。

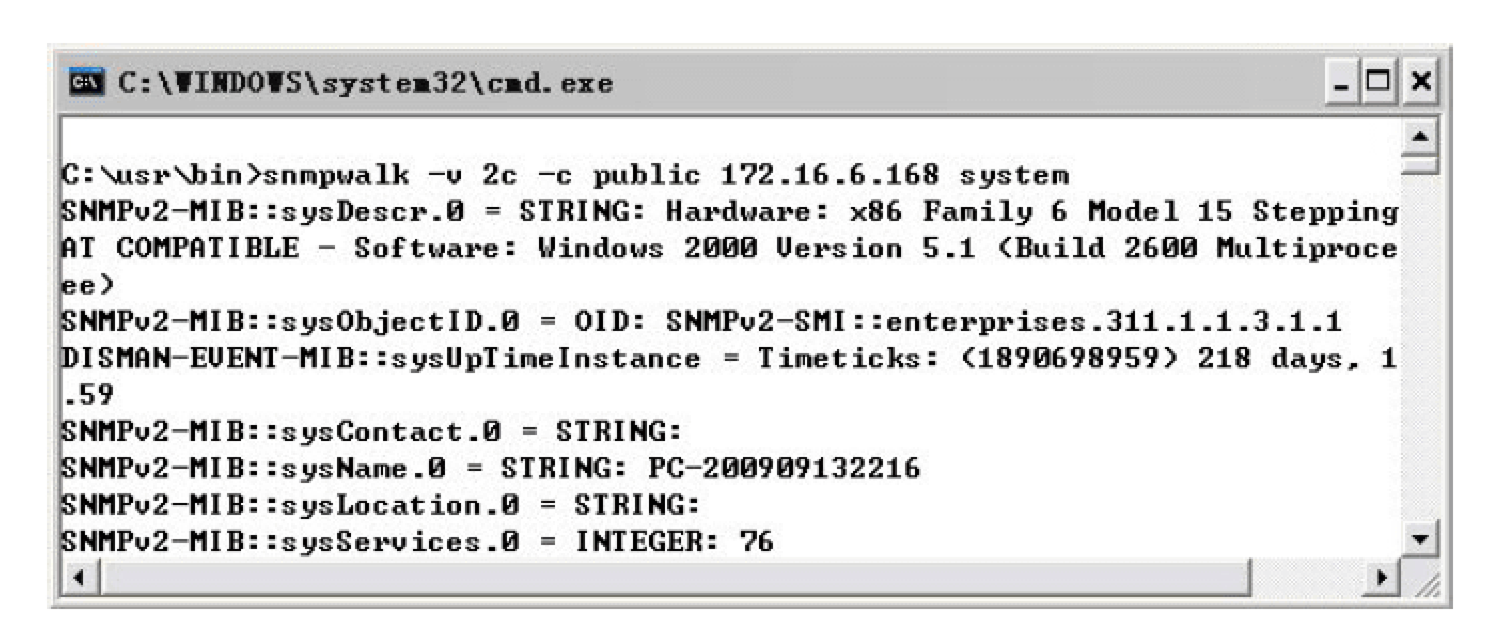


图 4-28　验证 SNMP 服务的运行状态

2．Net-SNMP 中提供的其他功能

Net-SNMP 除了提供 Agent 和 Trap 服务之外，还包含了一系列的软件工具包。使用这些命令工具，能够方便地进行网络设备管理，同时加深网管员对 SNMP 协议的理解和应用。这也是为什么要采用第三方代理程序的原因。Net-SNMP 提供的软件工具及其功能见 4.6。

表 4.6　Net-SNMP 中提供的工具包及其作用描述

序　号	名　称	作 用 描 述
1	snmpbulkget	模拟 SNMP 的 GetBulkRequest 操作，用来读取批量数据，代理会返回尽可能多的数据
2	Snmpbulkwalk	利用 GetBulkRequest 实现对指定 MIB 批量对象信息进行遍历读取
3	snmpd	SNMP 主代理程序，包括众多标准 MIB 的实现。还可以使用子代理对其进行扩展。在 Linux 和 Windows 系统运行 snmpd 后，系统便启动了对 SNMP 协议的支持
4	Snmpdelta	用来监测 SNMP 变量的改变，会及时报告值改变情况的工具
5	snmpdf	访问并检测显示实体对象的磁盘利用率
6	Snmpget	模拟 SNMP 的 GetRequest 操作，用来获取一个或多个 MIB 对象信息
7	Snmpgetnext	模拟 SNMP 的 GetNextRequest 操作，用来获取一个 MIB 对象信息的下一个可用对象数据

续表

序　　号	名　　称	作 用 描 述
8	Snmpnetstat	通过 SNMP 获取远程主机的网络状态和配置信息
9	Snmpset	模拟 SNMP 的 SetRequest 操作，用来设置一个或多个 MIB 对象为指定参数值
10	Snmpstatus	从 SNMP 实体中读取几个重要的信息对象以了解设备状态
11	snmptable	使用 GetNextRequest 和 GetBulkRequest 操作读取表信息，并以列表形式显示的工具
12	Snmptest	用于监测和管理网络实体的信息，通过 SNMP 请求操作与管理实体通信
13	Snmptranslate	将对象文本名称和标识符相互转化
14	Snmptrap	模拟发送 Trap 的工具
15	Snmptrapd	接收并处理 Trap 信息，一般用在代理的开发过程中，接收代理发来的 Trap，并显示数据包细节
16	snmpusm	用于配置 SNMP v3 USM
17	Snmpvacm	为一个网络实体创建或维护 SNMP v3 的基于视图访问控制参数的工具，用于维护 SNMP v3 的视图访问控制
18	Snmpwalk	对指定的管理树进行遍历
19	Snmpinform	模拟发送 InformRequest，用来发送模拟的带应答的 Trap，以测试管理站接收程序运行是否正常

Snmpwalk 命令在前面有过介绍。下面介绍其他几个较为常用的命令的简单用法，其详细的参数请查阅相关资料，此处不做详解。

Snmpget 命令：该命令语法与 Snmpwalk 相似，SNMP 版本、社区字符串和 OID 都是不可缺少的参数。例如，需要采集 sysDescr 的对象信息，sysDescr 的 OID 为 1.3.6.1.2.1.1.1.0，命令如图 4-29 所示。

```
C:\WINDOWS\system32\cmd.exe

C:\usr\bin>snmpget -c public -v 2c localhost 1.3.6.1.2.1.1.1.0
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 6 Model 15 Stepping 13
AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Multiprocesso
ee)
```

图 4-29　Snmpget 命令获取对象信息

Snmptranslate 命令：如果想要通过 MIB 中的对象文本描述串知道其 OID 值，或者通过 OID 值知道文本描述串，可以通过执行 Snmptranslate 来获取。例如，需要知道 SysName 的 OID 值，执行语句如图 4-30 所示。

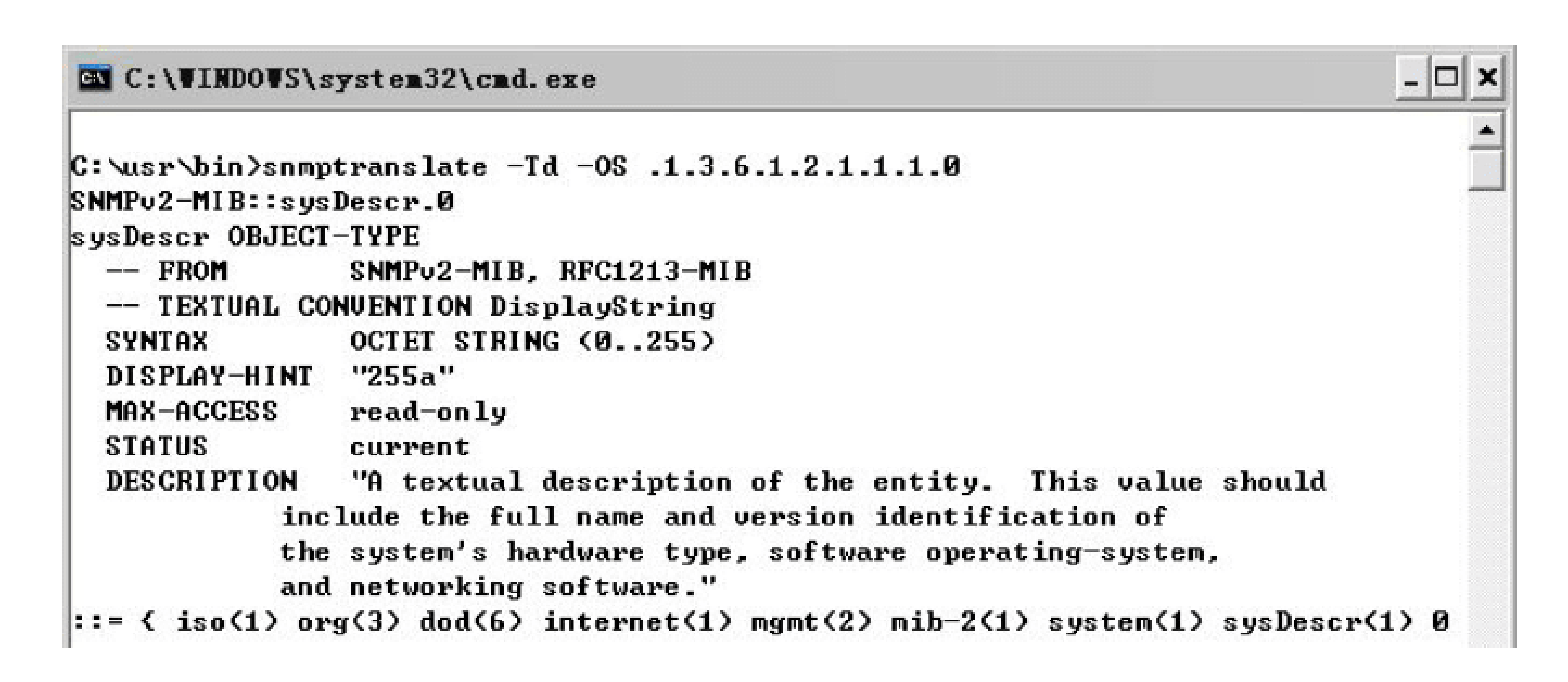
```
C:\WINDOWS\system32\cmd.exe

C:\usr\bin>snmptranslate -On -IR sysName
.1.3.6.1.2.1.1.5
```

图 4-30　Snmptranslate 命令示例

或者，通过 OID 值获得 sysdescr 的描述串，命令如图 4-31 所示。

如果想要了解系统状态，可使用 snmpstatus 命令，查询网络元素的一些重要统计信息，如各端口的状态、接收/发送数据包的总和等，如图 4-32 所示。



```
C:\usr\bin>snmptranslate -Td -OS .1.3.6.1.2.1.1.1.0
SNMPv2-MIB::sysDescr.0
sysDescr OBJECT-TYPE
  -- FROM       SNMPv2-MIB, RFC1213-MIB
  -- TEXTUAL CONVENTION DisplayString
  SYNTAX        OCTET STRING (0..255)
  DISPLAY-HINT  "255a"
  MAX-ACCESS    read-only
  STATUS        current
  DESCRIPTION   "A textual description of the entity.  This value should
                include the full name and version identification of
                the system's hardware type, software operating-system,
                and networking software."
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) system(1) sysDescr(1) 0
```

图 4-31　Snmptranslate 命令示例

```
C:\usr\bin>snmpstatus -c public -v 2c 172.16.6.168
[UDP: [172.16.6.168]:161]=>[Hardware: x86 Family 6 Model 15 Stepping 13 A
MPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Multiprocessor
Up: 4:29:14.31
Interfaces: 6, Recv/Trans packets: 793367/793750 | IP: 5151475/4444122
1 interface is down!
```

图 4-32　Snmpstatus 命令示例

4.3.4　在 Redhat Linux 服务器上开启 SNMP 服务

一般地，Linux 系统默认自带了 SNMP 代理程序，称为 Snmpd。该代理支持 SNMP v1、v2 和 v3 版本的网络管理协议。如果简单地选择使用 Linux 系统集成的 Snmp，可以使用命令 service snmpd start 和 service snmpd stop 分别来启动和停止服务。

在 Linux 中安装 SNMP 服务可以通过以下 3 种方式：

- ❑ 最初安装 Linux 的时候，选择安装 UCD-SNMP 和 SNMP-Utility 两个组件。
- ❑ 使用 RPM 包来安装。
- ❑ 使用第 3 方 SNMP 程序原代码进行安装。

下面详细介绍第 3 种安装方式。本书中推荐使用 Net-SNMP 代理程序，它实现了标准的 SNMP 协议，包括代理程序及附加 SNMP 工具。在其官方网站 www.net-snmp.com 上可下载各种版本的 Linux Net-SNMP 源代码，推荐下载文件名为 net-snmp-5.4.2.1.tar.gz 的 5.4.2.1 版本压缩包来进行安装。

以下以 Redhat Liunx 9 为例，介绍如何在文本模式下安装和开启 SNMP 服务。

（1）将下载的源代码包刻录到光盘中，通过光盘复制至 Linux 系统中进行安装，那么首先需要加载光盘文件。加载命令如下：

```
[root@tmp]#mount /dev/cdrom /mnt
```

进入到/mnt 目录，将看到目录中加载了 net-snmp-5.4.2.1.tar.gz 文件，该文件为压缩包，需要复制压缩包至系统中进行解压缩。将文件复制至/tmp 目录中的命令如下：

```
[root@mnt]#cp net-snmp-5.4.2.1.tar.gz /tmp_
```

（2）进入/tmp 目录中，使用 tar 命令对源代码包进行解压缩，会在当前目录生成文件

夹 net-snmp-5.4.2.1，并将文件解压至新建文件夹中。命令如下：

```
[root@tmp]#tar -zxvf net-snmp-5.4.2.1.tar.gz _
net-snmp-5.4.2.1/python/netsnmp/client.py
net-snmp-5.4.2.1/python/netsnmp/client_intf.c
net-snmp-5.4.2.1/python/netsnmp/tests/
net-snmp-5.4.2.1/python/netsnmp/tests/__init__
net-snmp-5.4.2.1/python/netsnmp/tests/test.py
net-snmp-5.4.2.1/python/netsnmp/tests/snmpd.co
net-snmp-5.4.2.1/python/LICENSE
```

然后进入到该文件夹即可看到包含的文件列表。命令分别如下：

```
[root@tmp]#cd net-snmp-5.4.2.1
[root@net-snmp-5.4.2.1]#ls
```

（3）执行文件目录下的 configure 可执行文件生成编译规则。如果需要指定程序的安装路径，则需要修改参数–prefix=/指定的路径名，此处指定安装在/usr/local/snmp 目录。命令如下：

```
[root@net-snmp-5.4.2.1]#./configure --prefix=/usr/local/snmp
```

命令执行结束后，可以看到编译规则的信息摘要如下：

```
---------------------------------------------------------
            Net-SNMP configuration summary:
---------------------------------------------------------

  SNMP Versions Supported:    1 2c 3
  Net-SNMP Version:           5.4.2.1
  Building for:               linux
  Network transport support:  Callback Unix TCP UDP
  SNMPv3 Security Modules:     usm
  Agent MIB code:             default_modules =>  snmpv3m
fication notification-log-mib target agent_mibs agentx di
ule utilities host
  Embedded Perl support:      enabled
  SNMP Perl modules:          building -- embeddable
  SNMP Python modules:        disabled
  Authentication support:     MD5 SHA1
  Encryption support:         DES AES

---------------------------------------------------------
```

（4）编译和安装 Net-SNMP，命令分别如下：

```
[root@net-snmp-5.4.2.1]#make _
```

```
[root@net-snmp-5.4.2.1]#make install_
```

在安装过程中会有如下提示，需要按照提示输入自定义的内容。

- Systemcontact information（配置该设备的联系信息）：manager（也可是邮箱地址）；
- System location（该系统设备的地理位置）：NANNING；
- Location to write logfile（日志文件位置）：/var/log/snmpd.log；
- Location to Write persistent（数据存储目录）：/var/net-snmp。

注意：在执行 make 命令的时候，可能会报错“no targets specified and no makefile found”。该提示为无法找到要编译的文件，也就是说 configure 没有正确生成 Makefile 文件。那么查看执行 configure 命令时的信息，如果包含“checking for gcc…no”，说明系统中没有 GCC 编译器，则需要下载安装包进行安装。

（5）编译安装完毕后，还需要将其配置文件（EXAMPLE.conf）复制至系统中进行配置。首先创建存放配置文件的目录/etc/snmp，然后将 net-snmp 解压文件目录（/tmp/net-snmp-5.4.2.1）中的 EXAMPLE.conf 复制到刚创建的目录/etc/snmp，并重命名为 snmpd.conf。命令分别如下：

```
[root@snmp]#mkdir /etc/snmp
```

```
#cp -R EXAMPLE.conf /usr/local/snmp/snmpd.conf
```

（6）编辑配置文件 snmpd.conf，更改其社区字符串和网络 IP 地址。命令如下：

```
[root@local]#vi snmpd.conf
```

在文件中查找到以下字段：

```
##          sec.name   source          community
#com2sec local       localhost       COMMUNITY
#com2sec mynetwork NETWORK/24      COMMUNITY
```

将 community 字段改为要设置的密码，例如 public。把 NETWORK 改成需要查看该设备 snmp 信息的网络来源 IP（172.16.6.168）地址，或改为本机地址，如下：

```
##          sec.name   source          community
com2sec  local       localhost       COMMUNITY
com2sec  mynetwork 172.16.6.168    public
```

（7）启动 snmpd 进程。

```
#/usr/local/snmp/sbin/snmpd -c /etc/snmp/snmpd.conf
```

使用 snmpd 命令启动 snmp 进程，前半部分路径为 Net-SNMP 的安装目录，后半部分路径为配置文件所在的位置，也就是 snmpd.conf 文件存放的路径。执行启动命令后，可使用 ps 命令查看 snmpd 进程是否已启动。命令如下：

```
[root@root]#ps -aux|grep snmpd
root      1983  0.0  1.7 10036 4420 ?       S    10:04   0:00 usr/local/snmp/sb
```


此时可以看到 SNMP 进程已经正常启动，此外，还需要将第 7 步的启动命令写入文件 /etc/rc.local 末尾，以确保每次重启 Linux 后都能自动启动 SNMP 服务。编辑 rc.local 文件的命令如下：

```
[root@local]#vi /etc/rc.local
```

如果需要停止 Net-SNMP 服务，则需要使用 Kill -9 [SNMP 进程 ID]命令。如下：

```
[root@snmp]#kill -9 1983
```

（8）安装完成后，通过命令本地测试 Snmpd 服务，查看服务是否正常运行。使用 Snmpwalk 命令可用来查看 MIB 对象，在不加具体 OID 参数时，Snmpwalk 将遍历获取本机中所有的 MIB 对象，执行如下命令：

```
#snmpwalk -v 2c -c public serverIP
```

此处 serverIP 为测试对象 IP 地址，更改为本机 IP 即可。如果 Snmpd 运行正常，则会显示如下信息：

```
[root@snmp]#snmpwalk -c public -v 2c 172.16.6.170 | more
SNMPv2-MIB::sysDescr.0 = STRING: Linux RedhatServer 2.4.20
:28 EST 2003 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgen
SNMPv2-MIB::sysUpTime.0 = Timeticks: (14919) 0:02:29.19
SNMPv2-MIB::sysContact.0 = STRING: Me <me@somewhere.org>
SNMPv2-MIB::sysName.0 = STRING: RedhatServer
SNMPv2-MIB::sysLocation.0 = STRING: Right here, right now.
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (28) 0:00:00.28
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrame
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDComplian
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMI
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
```

如果需要通过远程主机来查看该 Redhat Linux 中的 MIB 信息时，还需要查看该 Linux 服务器是否打开了 UDP 161 端口。通过 netstat –ln 命令可查看 161 端口是否打开了，命令如下：

```
[root@snmp]#netstat -an | grep 161
udp        0       0 0.0.0.0:161            0.0.0.0:*
```

如果没有开启，则开启命令如下：

```
[root@root]#ns -lp 161 &
```

开启端口后，可在远程主机中使用该命令或第三方 MIB 浏览工具来进行测试。

（9）如果需要配置 Linux 主机自动发送 Trap 消息至网管主机（172.16.6.168），那么需要在 snmpd.conf 文件中添加如下内容：

```
# send v1 traps
trapsink   192.168.6.168:162 public
# also send v2 traps
trap2sink   192.168.6. 168:162 public
informsink  192.168.6. 168:162
```

添加完成后，需要重启 Snmptrapd 服务。命令如下：

```
[root@RedhatServer/]#snmptrapd -d -f
Starting snmptrapd 5.0.6
```

如果需要停止 Snmptrapd 服务，则使用如下命令：

```
[root@RedhatServeretc]#service snmptrapd stop
Stopping snmptrapd:
```

通过以上命令，完成了在 Redhat Linux 中的配置和启动 Net-SNMP 相关服务。

4.3.5 Trap 信息的发送和接收验证

Trap 的验证需要 Agent 和 Manager 两端的配合。此处以 Redhat Linux 服务器为 SNMP Agent 端，以 Windows XP 管理主机为 SNMP Manager 端，通过在 Linux 系统中使用 Net-SNMP 的 Trapd 服务发送陷井消息。相应地，在 Windows 主机中同样使用 Net-SNMP 的 Trapd 服务来接收消息。此处的主要目的是验证 Linux 客户端 Trap 消息的发送和 Windows 服务器端接收消息是否正常，以及了解 Trap 消息的机制。

在后面的章节中介绍的网管软件，也用到了 Trap 消息的监测方式，并且能够获得更为直观的信息。验证 Trap 消息操作步骤如下：

（1）在 Windows 系统中配置 Net-SNMP 监听和接收远程 Trap 消息，在 CMD 命令窗口中进入到 Net-SNMP 安装目录（C:\Usr\bin），开启对 Snmptrapd 工具对端口 162 的 Trap 消息监听。命令如图 4-33 所示。

```
C:\WINDOWS\system32\cmd.exe - snmptrapd -f -Le -d

C:\usr\bin>snmptrapd -f -Le -d
Warning: no access control information configured.
This receiver will *NOT* accept any incoming notifications.
NET-SNMP version 5.4
```

图 4-33　打开 Net-SNMP 的 Trap 消息监听服务

此时，将会看到错误提示 Not accept any incoming notifications。也就是说，Net-SNMP 目前仍无法接收到任何的 Trap 消息，因为还需要授权接收 Trap 消息的种类。

对于网管主机，如果开启了 Trap 监听，将会收到来自网络设备大量的 Trap 消息，例如系统重启、接口中断、接口恢复连接等。其中只有少量的信息是有用的，所以默认的，Windows 下 Net-SNMP 程序不接收任何类型 Trap 消息，除非提供了专门的授权。此处授权 Net-SNMP 接收所有的 Trap 消息。需要在 C:\usr\bin 目录下，建立一个授权文件，命名为 snmptrapd.conf，并在其中写入语句 DisableAuthorization yes，然后在命令中读取该文件中的授权参数，命令如图 4-34 所示。



图 4-34　授权 Net-SNMP 的 Trap 服务接收全部消息

此时，Snmptrapd 功能已经启用，Net-SNMP 开始监听 162 端口并准备处理接收到的 Trap 消息。

（2）配置 Trap 消息发送端。在 Linux 中，通过命令 Snmptrap 发送 Trap 测试消息，命令格式如下：

```
snmptrap [ -a Host ] [ -c Community ] [-d ] -m Message
```

命令参数：

- -a Host，指定发送对象的 IP 地址。
- -c Community，连接的社区字符串。
- -d，启用调试工具。
- -m Message，snmptrap 命令要发送的消息。

发送 Trap 消息的示例命令如下：

```
# snmptrap -v 2c -c public 172.16.6.168:162 "" UCD-SNMP-MIB::ucdStart
```

输入该命令并按回车键后，若 Redhat Linux 不会有任何提示，则命令已正常执行。

（3）此时，回到 Windows 界面中的 CMD 命令窗口，可以看到 snmptrapd 监听界面中已经接收到了 Trap 数据包，并将数据包内容进行尽可能的展开，如图 4-35 所示。

```
C:\WINDOWS\system32\cmd.exe
C:\usr\bin>snmptrapd -c "c:\usr\bin\snmptrapd.conf" -f -Le -d
NET-SNMP version 5.4

Received 73 bytes from UDP: [172.16.6.168]:34140
0000: 30 47 02 01  01 04 06 70  75 62 6C 69  63 A7 3A 02    0G.....public.:.
0016: 04 6D 81 26  85 02 01 00  02 01 00 30  2C 30 10 06    .m.&.......0,0..
0032: 08 2B 06 01  02 01 01 03  00 43 04 46  57 9D D9 30    .+.......C.FW..0
0048: 18 06 0A 2B  06 01 06 03  01 01 04 01  00 06 0A 2B    ...+...........+
0064: 06 01 04 01  8F 65 81 7B  01                          .....e.{.

2009-12-18 11:49:54 <UNKNOWN> [UDP: [172.16.6.168]:34140]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1180147161) 136 days, 14:11:11
.61      SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::ucdStart
```

图 4-35　Net-SNMP 接收到的 Trap 消息报文

此处收到的 Trap 消息数据包内容较难读懂。在后续章节中介绍的 WhatsUp Gold 网管程序中将能够直观明了地展示接收到的 Trap 消息内容。

4.3.6 H3C 网络设备的 SNMP 服务配置

H3C 交换机和路由器对 SNMP 服务的开启命令是相同的。不同的地方在于，当配置设备发送 Trap 消息时，需要指定设备的一个端口作为消息发送的源地址。交换机和路由器的端口选择是有分别的，具体设置将分别讲解。首先介绍在 H3C 交换机和路由器中配置 SNMP 服务。

配置内容包括启动和关闭 Snmp Agent 服务、设置 Snmp 组、管理员的联系方式、允许和禁止发送 Trap 报文、设置 Trap 消息目标主机的 IP 地址、指定发送报文的源地址等。设置步骤如下：

（1）使用命令 System-View 进入到交换机配置视图中。命令如下：

```
<H3C>system-view
```

（2）默认情况下，SNMP Agent 服务处于关闭的状态，可使用如下命令启动该服务。启用 agent 服务命令如下：

```
[H3C]snmp-agent
```

关闭 agent 服务命令如下：

```
[H3C]undo snmp-agent
```

（3）设置系统信息，主要是设置管理员联系方式和设备物理地址。命令格式如下：

```
snmp-agent sys-inf contact {syscontact} location {sys_location}
```

例如，设置管理员韩先生的地址，如下：

```
[H3C]snmp-agent sys-info contact Mr.Han location  3rd floor
```

（4）如果要启用指定版本的 SNMP 协议（可指定 1 个或多个），命令格式如下：

```
snmp-agent sys-info version {[v1|v2c|v3]|all}
```

例如，设置该交换机使用 v1 和 v2c 版本，如下：

```
[H3C]snmp-agent sys-info version v1 v2c
```

如果无法确定，推荐设置为 all 以支持 3 个协议版本，如下：

```
[H3C]snmp-agent sys-info version all
```

（5）设置社区字符串及访问权限，命令格式如下：

```
snmp-agent community {read|write community-name}
```

例如，设置 public 为读字符串，如下：

```
[H3C]snmp-agent community read public
```

例如，设置 private 为写字符串，如下：

```
[H3C]snmp-agent community write private
```

4.3.7 配置 H3C 交换机发送 Trap 消息

（1）配置交换机允许发送 Trap 报文，配置命令格式如下：

```
snmp-agent trap enable standard [authentication|cold start|linkdown|linkup]
```

参数：

Standard，发送 SNMP 标准的通知或 trap 信息，见表 4.7。

表 4.7 交换机 Trap 报文的参数

序 号	参数名称	参数描述
1	Authentication	认证失败时，发送 SNMP 的认证 Trap 信息
2	Coldstart	交换机重启时，发送冷启动 Trap 信息
3	Linkdown	交换机端口为 Down 时，发送链路断开的 Trap 信息
4	Linkup	交换机端口为 Up 时，发送链路连接的 Trap 消息

如果不带参数，表示发送所有模块的所有类型的 Trap 报文。如果只需要发送部分类型的 Trap 报文，则相应地加入参数。

例如，需要发送 Link 状态变化及系统重启的 Trap 报文，命令为 snmp-agent trap enable standard linkdown linkup coldstrat，如下：

```
[H3C]snmp-agent trap enable standard linkdown linkup coldstart
```

禁止 trap 服务的命令为 undo snmp-agent trap enable strandard。

（2）在配置模式中，设置发送 Trap 消息的目标主机地址，命令格式：

```
snmp-agent target-host trap address udp-domain {host-addr} udp-port
[udp-portnumber] params securityname  [security-string]  [v1|v2c|v3]
```

命令参数：

- ❑ host-addr，目标主机 IP 地址。
- ❑ udp-portnumber，接受 Trap 消息的主机 UDP 端口号。
- ❑ community-string，访问社区字符串。

例如，设置向目标地址为 172.16.6.168 发送 Trap 消息，社区字符串为 public，命令格式：

```
snmp-agent target-host trap address udp-domain 172.16.1.1 udp-port 162
params securityname public v2c
```

如下：

```
   [H3C]snmp-agent target-host trap address udp-domain 172.16.6.168 udp-port
5000 params securityname public v2c
```

如需取消向目的地址发送 Trap 消息，则命令格式为 undo snmp-agent target-host。

注意：以上设置步骤，对于 H3C 品牌的交换机和路由器均为一致的。在下一步骤，为防止 Trap 消息的发送泄露了端口 IP 地址信息，需要设置设备的某 IP 地址作为 Trap 报文发送源地址，该地址设置对于交换机和路由器设置方式略有不同。

（3）设置某 IP 地址为发送 Trap 消息的源地址，命令格式如下：

```
Snmp-agent trap source interface-type {interface-number | interface-number.
subnumber}
```

在路由器中，可将某端口地址（如 GigabitEthernet 1/0）作为源地址。而在交换机中，需要设置某 Vlan IP 地址作为发送 Trap 的源头地址，可将 Valn 地址（如 Vlan-interface 2）作为源地址。

例如，在交换机的配置模式下，建立 vlan 并设置 IP 地址，命令如下：

```
[H3C]vlan 2
[H3C-vlan2]port ethernet 1/0/2
[H3C-vlan2]quit
[H3C]interface vl
[H3C]interface Vlan-interface 2
[H3C-Vlan-interface2]ip address 172.16.6.1 255.255.0.0
[H3C-Vlan-interface2]quit
```

之后，将该地址设置为 Trap 源地址，命令为 snmp-agent trap source vlan-interface 2，如下：

```
[H3C]snmp-agent trap source Vlan-interface 2
```

4.3.8 查看 H3C 交换机 Snmp 信息

（1）显示报文信息命令为 Display snmp-agent sys-info [contace | location | version]，如下：

```
[H3C]display snmp-agent sys-info
   The contact person for this managed node:
           Mr.Han location  3rd floor

   The physical location of this node:
           Hangzhou China

   SNMP version running in the system:
           SNMPv1 SNMPv2c SNMPv3
```

（2）显示配置的社区名信息命令为 Display snmp-agent community [read | write]，如下：

```
[H3C]display snmp-agent community
   Community name:public
       Group name:public
       Storage-type: nonVolatile

   Community name:private
       Group name:private
       Storage-type: nonVolatile
```

（3）显示当前的 MIB 视图命令格式为 display snmp-agent mib-view。

4.4 WMI 概念和介绍

WMI（Microsoft Windows Management Instrumentation，Windows 管理规范）是 Microsoft

针对 Windows 操作系统的核心管理支持技术，是从 Windows 系统中提取信息的标准。WMI 默认安装于 Windows 2000/2003/XP 系统，只要网管员管理 Windows 服务器和工作站，或者需要创建 Windows 管理应用程序，就需要了解 WMI。在后续章节介绍的网管程序中，也应用了 WMI 方式采集 Windows 系统的性能参数。

在 WMI 技术出现之前，如果需要用编程实现对 Windows 信息的配置和管理，那么开发工具均需要调用 Win32 的应用 API（Application Programming Interface，程序编程接口）。API 是应用程序与 Windows 系统结构相互通信的唯一桥梁。但 WMI 技术出现之后，系统管理员可以通过简单的脚本语言，即可实现常用的系统管理任务（WMI 提供了对 VB、WSH、VBScirpt、JScript、ASP 脚本语言的支持）。

4.4.1 WMI 的功能介绍

利用 WMI 可以高效地管理远程和本地的计算机，通过它可以访问、配置、管理和监测任何通过 WMI 公开的 Windows 资源。比如管理员可使用 WMI 脚本库创建系统管理脚本，使用 Windows Script Host 和 Microsoft Visual Basic Scripting Edition（VBScript）或任何支持 COM 自动化的脚本语言（例如 ActiveState Corporation 的 ActivePerl），来管理和配置操作系统、应用程序和网络的下列方面。

Windows Server 2003、Windows XP 专业版和 Windows 2000 系统管理：网管员可以编写脚本来检索性能数据，管理事件日志、文件系统、打印机、进程、注册表设置、计划程序、安全性、服务、共享及很多其他的操作系统组件和配置设置。

网络管理：可以创建基于 WMI 的脚本来管理网络服务，例如 DNS、DHCP 和启用 SNMP 的设备。

实时健全监测：使用 WMI 事件订阅，可以编写代码以在事件发生时监测并响应事件日志项，监测并响应文件系统、注册表修改及其他实时的操作系统更改。

4.4.2 WMI 监测与 SNMP 监测的区别

WMI 监测方式不同于 SNMP 监测。WMI 监测的内容由 Windows 操作系统定义，其获取的是 Windows 系统所管理的信息，包括系统进程、Windows 应用程序等。而 SNMP 监测方式具备更多的通用性，除 Windows 操作系统外，还能获取包括网络、Linux 系统、传输协议等方面的信息。

该两种监测方式获取的信息对象包含重叠的部分。例如，获取 Windows 磁盘利用率、硬件属性、系统进程等，两种方式都能够采集到同样的信息。实际应用中，可根据需要或熟悉程度进行选择。

一般地，在采集性能数据时没有必要使用 WMI 方式，除非 Windows 设备不支持 SNMP，或者需要通过 WMI 在不支持 SNMP 管理的设备中采集信息，那么可以通过在性能监测库中建立自定义的 WMI 性能监测功能。

4.4.3 WMI 体系结构

WMI 体系结构由 3 个部分组成：托管资源、WMI 基础结构和使用者。分别介绍如下。

1. 托管资源

托管资源是任意程序或实体组件，可通过使用 WMI 进行管理。可以使用 WMI 管理的 Windows 资源包括操作系统、磁盘、其他硬件设备、日志记录、文件系统、网络组件、性能计数器、打印机、服务进程、注册表、安全配置、共享管理及应用程序等。WMI 托管资源通过一个提供程序与 WMI 通信。

2. WMI 基础结构

WMI 由 3 个主要组件构成：CIMOM（Common Information Model Object Manager，公共信息模型对象管理器）、CIM（Common Information Model，公共信息模型储存库）及提供程序。这 3 个 WMI 组件共同定义和组成了其基础结构，可通过该结构定义、公开、访问、检索配置和管理数据。该 3 个组成部分结构，如图 4-36 所示。

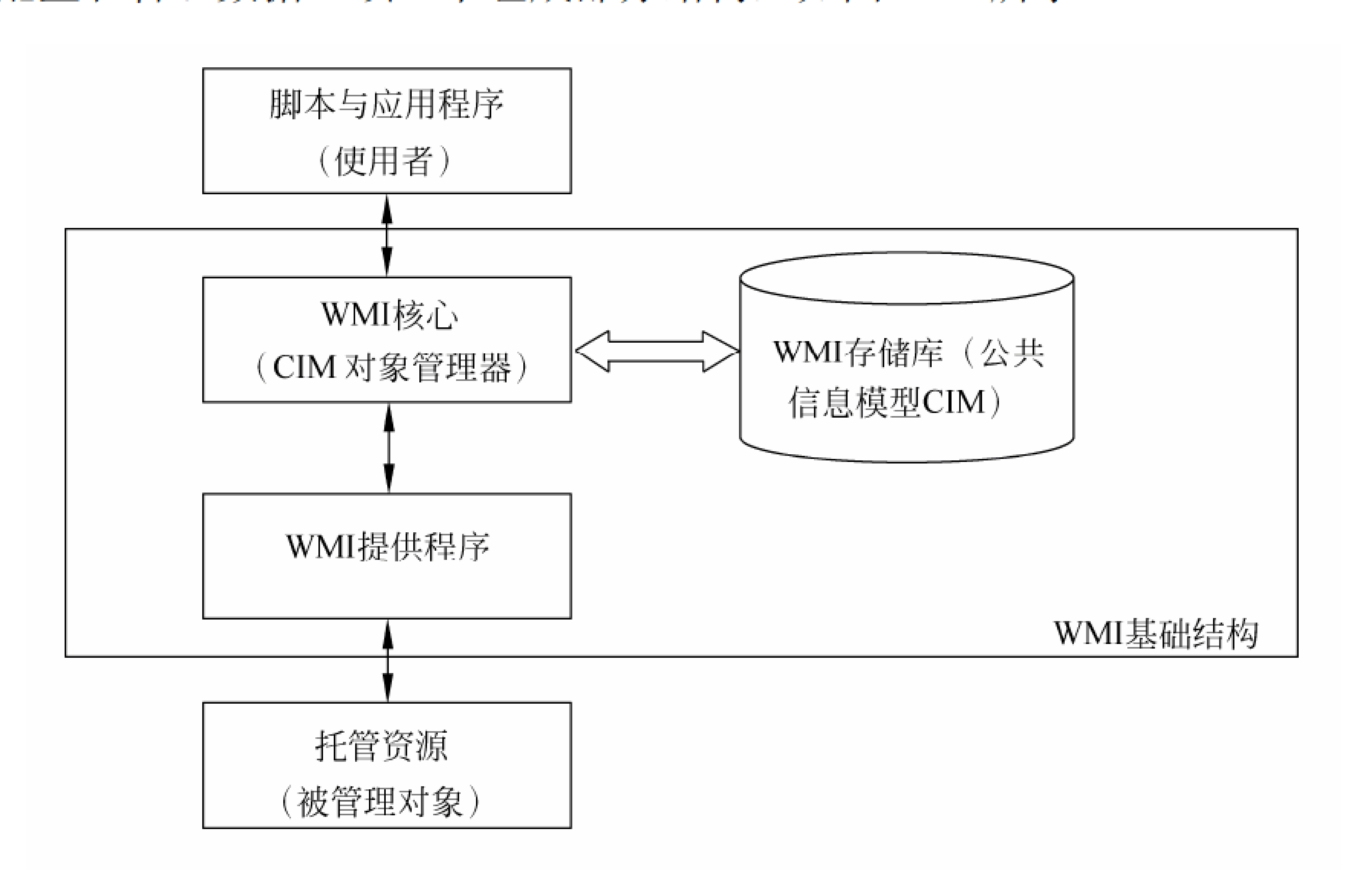


图 4-36　WMI 体系结构

3. 使用者

包括所有调用 WMI 类别的程序、网管系统和简单脚本语言。

4.4.4 WMI 包含的类别

如果要利用 WMI 管理 Windows 系统，那么熟悉 WMI 类别是非常重要的。WMI 定义了如表 4.8 所示的类别，每一个类别中包含若干的实例对象。需要了解类别的详细内容，

请查阅相关资料。类别的简单描述和举例如表 4.8 所示。

表 4.8　WMI 类别描述

WMI 类别	描　述	类别对象举例
Win32 类别	这是处理 Windows 操作系统最重要的类别，包括硬件管理、服务、进程、性能计数器等	Win32_Process：进程 Win32_Service：服务 Win32_PhysicalMemory：物理内存
WMI Registry 类别	用来编辑、新增、删除 Windows 注册表项目和键值的类别	Win32_Registry--注册表
WMI System 类别	只要是以两个下划线“__”开头的名称，就属于该类别，这些类别为 WMI 提供了许多基本功能	__Event 事件 __TimerEvent 时间类事件
WMI System 属性	这些属性主要用于 WMI 的内部运作，这些属性的名称也可以是以两个下划线作为开头的名称	__SystemEvent 系统事件 __SystemSecurity 系统安全性
MSFT 类别	由微软提供的用于处理其他系统作业功能的类别	MSFT_WmiCoreUser 核心用户 MSFT_WmiCoreLogonEvent 核心用户登录事件
CIM 类别	如果想要开发 WMI 类别，就可以从该类别继承。Win32 类别就是从该类继承	CIM_AlarmDevice 报警装置 CIM_Process 进程
Standard Consumer 类别	一组会触发特定事件的 WMI 事件使用者	__ConsumerFailureEvent 应用失败事件
MSMCA 类别	处理系统事件的类别	微软已建议不使用
WMI C++类别	WMI C++ Provider Framework 类别	微软已建议不使用

4.4.5　WMI 应用工具 WMI Explorer 介绍

在通过 SNMP 协议查看 MIB 对象时，可方便地使用可视化工具 MIB Browser 进行浏览。同样也有类似的工具用于查看 WMI 对象。免费的 WMI 浏览工具 WMI Explorer 就能够方便地查看本机和远程主机的 WMI 信息。

WMI Explorer 下载之后不需要安装，直接运行即可，主界面如图 4-37 所示。

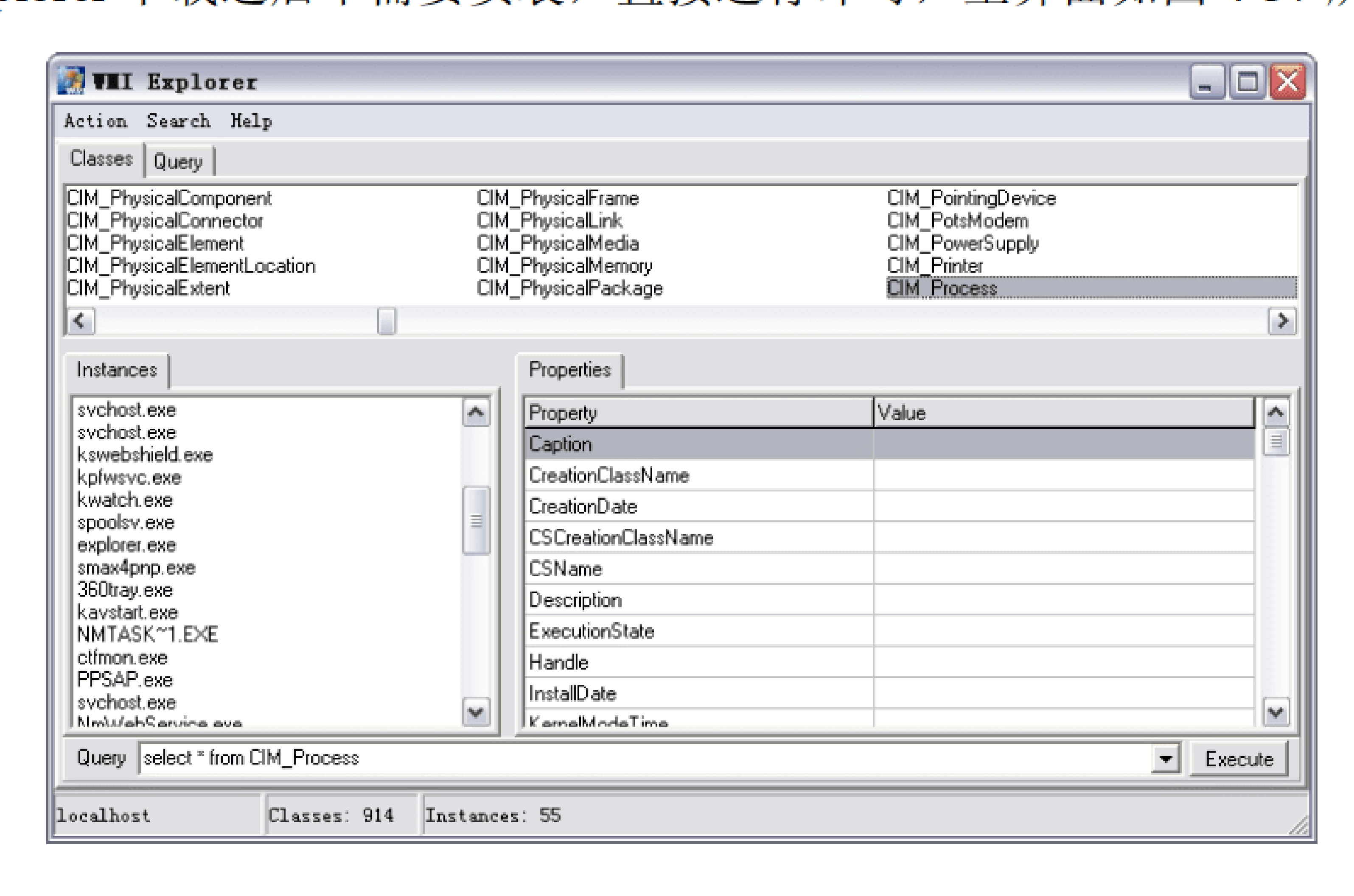


图 4-37　WMI Explorer 主界面

以下对 WMI Explorer 的界面及功能进行介绍。

1. Classes 选项页

在界面上方部分，列出了系统中可用的所有 WMI 类别。为了能够快速查找到目标对象，可以使用菜单命令 Search 下的 Find 子菜单命令，并输入类别的名称进行查询，使用菜单命令 Search Again 可查找下一目标对象。

例如，输入_Process 查找到的对象包括 CIM_Process、CIM_ProcessExecutable、CIM_Processsor、CIM_ProcessThread、Win32_Process 和 Win32_Processor。查找方式如图 4-38 所示。

2. Instrance 选项页

在该界面的左下方，列出了所选 WMI 类别中所包含的实例，每次选择一个 Classes 类别时，该面板中将显示其对应的实例内容。值得注意的是，有的 WMI 类别包含大量的 Instance 对象，列出了对象需要耗费较长的时间和占用较多内存。CIM 进程的实例内容如图 4-39 所示。

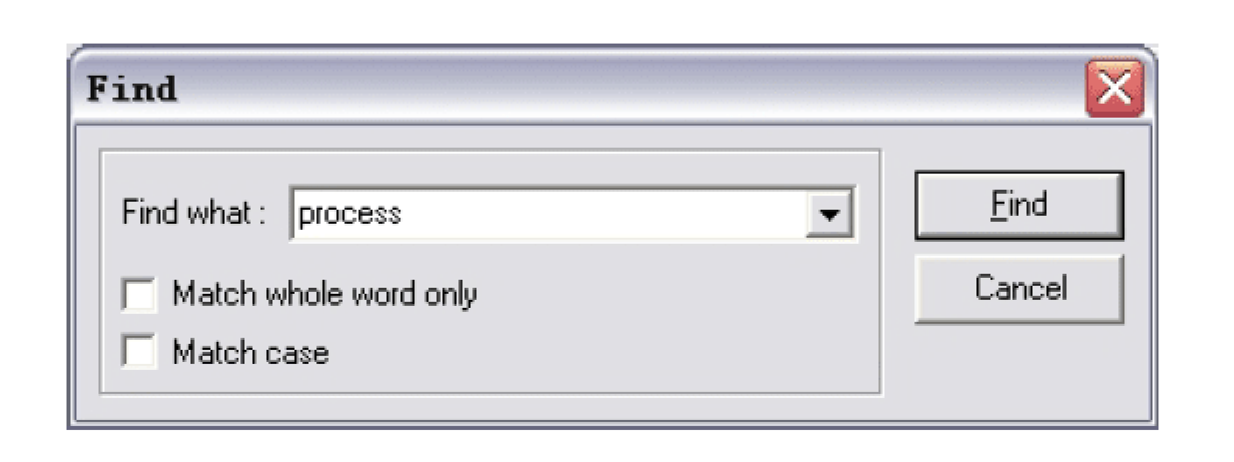


图 4-38　查找 Classes 对象

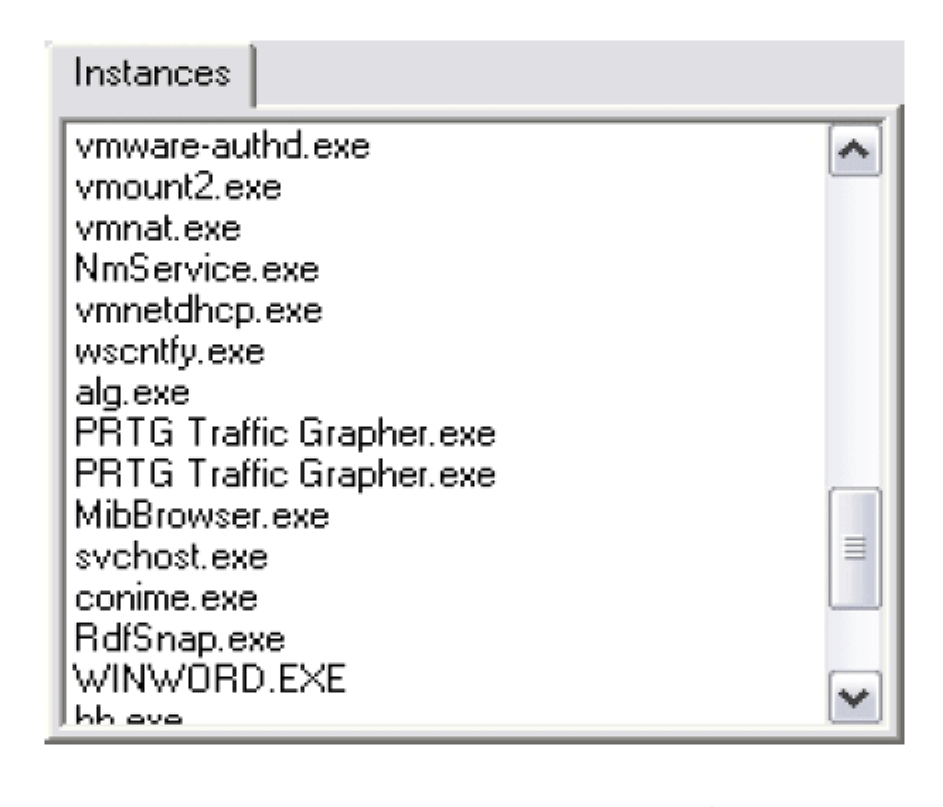


图 4-39　CIM 进程的 Instance 实例列表

3. Properties 选项页

在界面的右下方，列出了所选 Instance 实例的属性，如 Name、Version、Status 等属性。选择进程中的实例 WINWORD.EXE 进程，即可看到该实例所包含的各类属性，包括其路径、句柄、版本等各类信息，如图 4-40 所示。

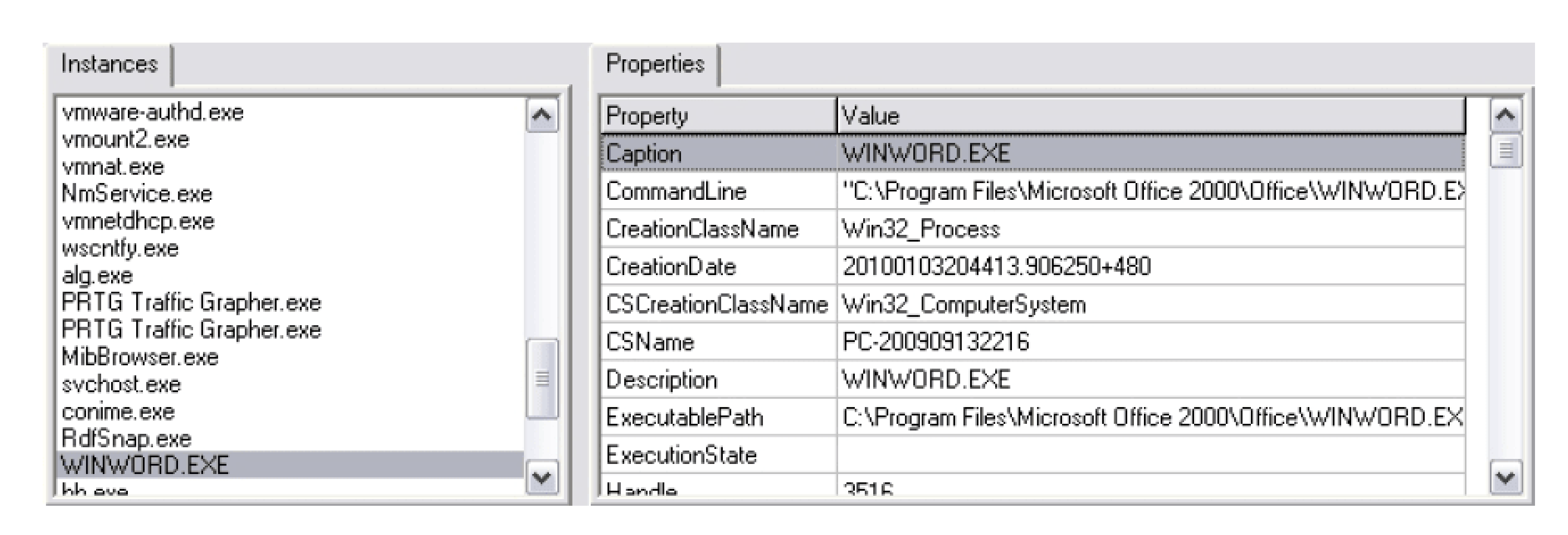


图 4-40　Word 进程的属性

4．查询实例功能

在主界面的 Query 文本框中，提供了执行标准 WMI 查询语句 WQL（WMI Query Language）的功能，可查询到 WMI 类别中所包含的实例及其属性信息。其语句的语法类似于 SQL 语言。例如，查询 CIM 类别中的进程，可使用语句“SELECT*FROM CIM_Process”，单击 Execute 按钮，即列出了所有的进程，如图 4-41 所示。

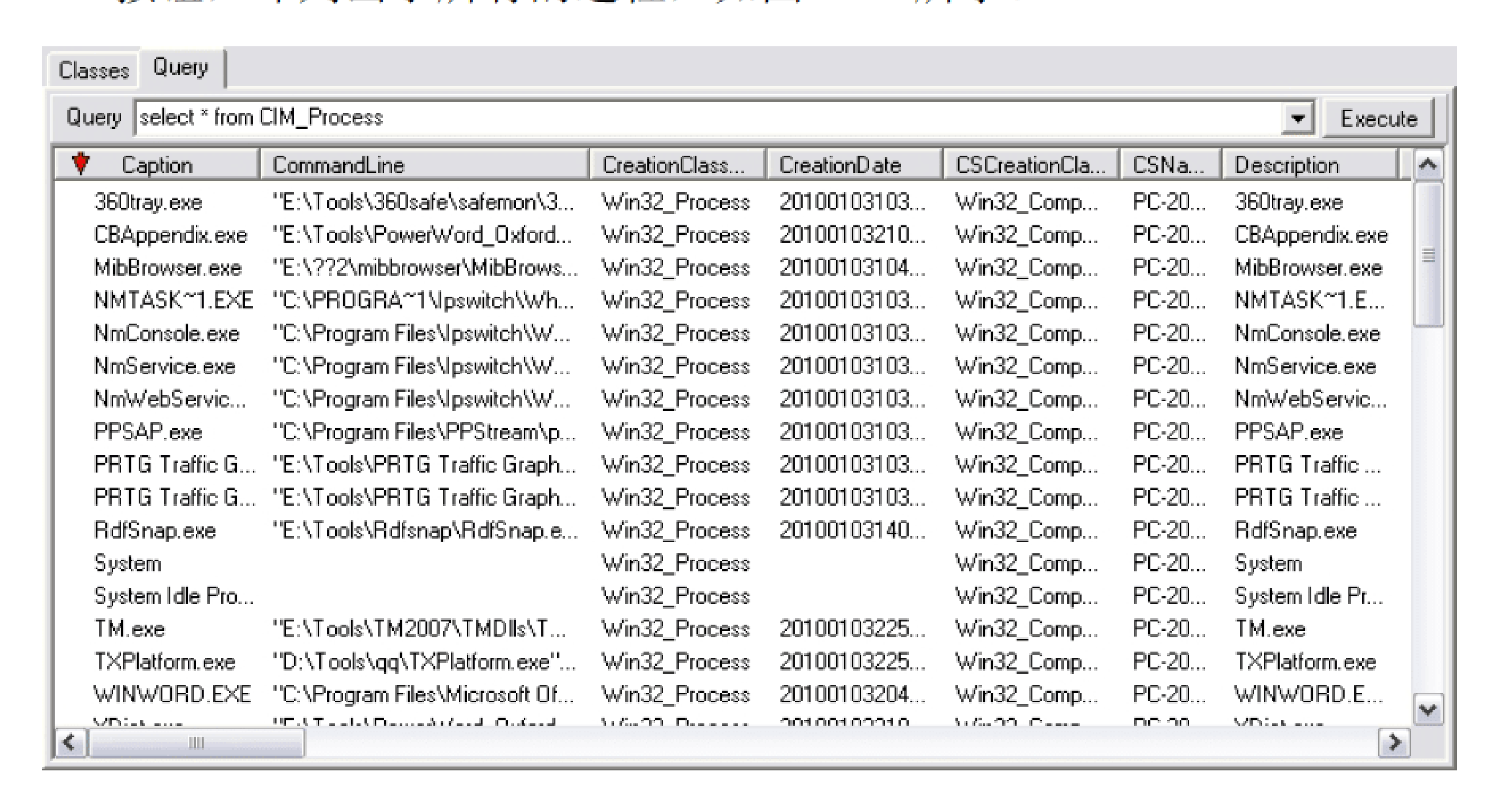


图 4-41　查询到的 CIM 进程列表

关于 WMI Explorer 更详细的功能介绍和应用请查阅相关的帮助文档。

4.4.6　WMI 的简单操作命令

Windows 操作系统中默认提供了非常方便的 WMI 管理工具—WMIC（Windows Management Instrumentation Command-line，Windows 管理规范命令行）。使用 WMIC，不仅可以管理本地计算机，只要有域用户的登录权限，还可实现对域内远程计算机的管理。

执行【开始】|【运行】命令，输入 CMD 打开命令提示符，并输入 wmic.exe。如果是首次使用该工具，系统会提示安装 WMIC。自动安装结束后，则会出现该工具的命令提示符：wmic：root\cil>，此时可以使用一些配置命令实现对计算机的控制。下面简单介绍几个命令来说明 WMI 的应用。

- 了解系统当前服务进程，命令格式为 wmic process list m，m 是进程列表的参数，m 取值为 brief 时命令将显示当前进程的主要（摘要）信息，包括名称、进程 ID、占用内存情况等。m 取值为 system 时，命令将只显示系统进程的参数值；m 取值为 full，则命令将获取完整的进程信息。使用命令 process list brief，如图 4-42 所示。
- 显示 CPU 的时钟频率，命令为 path win32_processor get maxclockspeed，命令将显示计算机 CPU 当前运行的始终频率值。
- 查看 BIOS 信息，命令为 bios list full。

```
C:\WINDOWS\system32\cmd.exe - wmic
wmic:root\cli>process list brief
HandleCount  Name               Priority  ProcessId  ThreadCount  WorkingS
0            System Idle Process  0       0          2            16384
787          System               8       4          81           286720
19           smss.exe             11      1300       3            434176
733          csrss.exe            13      1352       12           17530880
401          winlogon.exe         13      1376       25           3358720
349          services.exe         9       1424       16           3948544
400          lsass.exe            9       1436       21           1970176
36           ibmpmsvc.exe         8       1604       6            1626112
221          svchost.exe          8       1632       19           5537792
362          svchost.exe          8       1680       11           4923392
1638         svchost.exe          8       252        75           25178112
64           btwdins.exe          8       332        5            2764800
92           svchost.exe          8       864        6            4370432
```

图 4-42　Process 命令查看系统进程

- ❑ 获取账户信息，命令为 useraccount list brief。
- ❑ 列出帮助文件，命令格式为/?，执行结果如图 4-43 所示。



图 4-43　Wmic 帮助命令

4.4.7　利用 WMI 执行脚本命令

实例 1：确定计算机 IP 地址，脚本内容如下：

```
strComputer = "."
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
Set IPConfigSet = objWMIService.ExecQuery _ ("Select IPAddress from
              Win32_NetworkAdapterConfiguration where IPEnabled=TRUE")
For Each IPConfig in IPConfigSet
    If Not IsNull(IPConfig.IPAddress) Then
        For i=LBound(IPConfig.IPAddress) to UBound(IPConfig.IPAddress)
            WScript.Echo IPConfig.IPAddress(i)
    Next
    End If
Next
```

将脚本内容保存到磁盘中（例如 C:\目录下）的 Text 文本中，并将文本文件改名为 GetIp.vbs，然后在 CMD 命令窗口中输入“C:\>cscript Getip.vbs”，则调用执行该脚本文件，并得到操作系统的版本信息。命令执行结果如图 4-44 所示。

实例 2：识别操作系统，脚本如下：

```
strComputer = "."
```

```
Set objWMIService = GetObject ("winmgmts:" & "{impersonationLevel=impersonate}!\\"
                    & strComputer & "\root\cimv2")
Set colOperatingSystems = objWMIService.ExecQuery _
                    ("Select * from Win32_OperatingSystem")
For Each objOperatingSystem in colOperatingSystems
    Wscript.Echo objOperatingSystem.Caption & " " & objOperatingSystem.Version
Next
```

同样将上述脚本保存到 Text 文件中，并重命名为 getsystem.vbs，执行该脚本文件后即得到系统的版本信息。命令执行结果如图 4-45 所示。

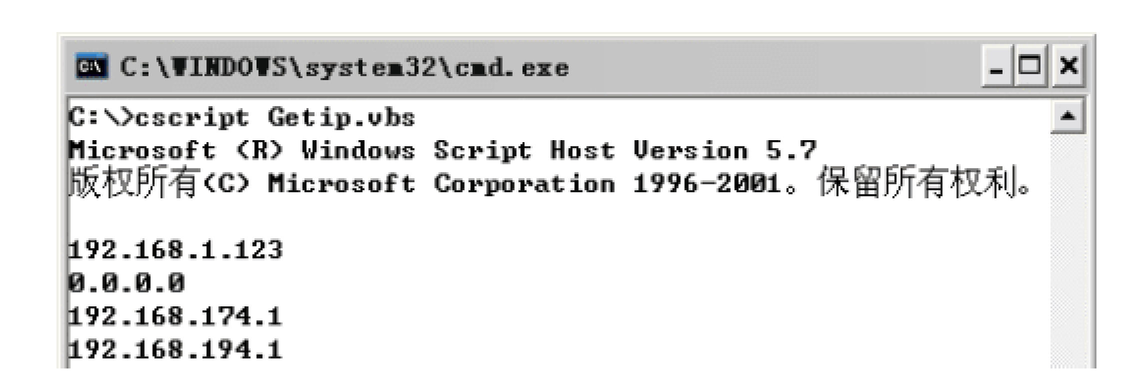


图 4-44 执行获取 IP 地址的脚本命令

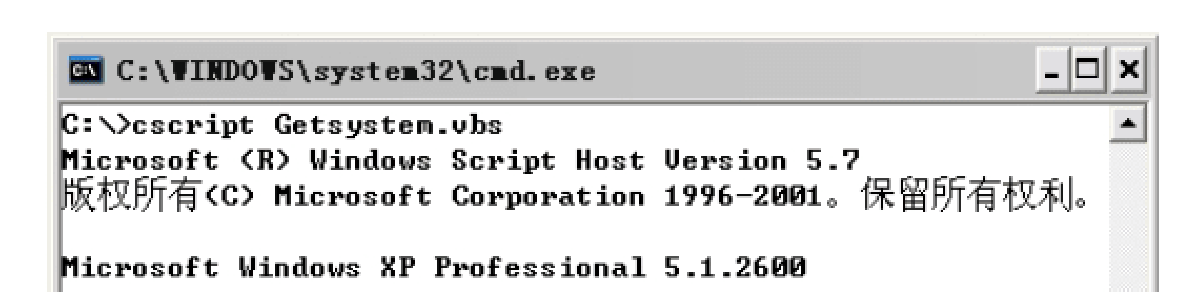


图 4-45 执行获取版本信息的脚本命令

访问 Microsoft 官方网站的脚本中心，可获取更多的应用脚本。

4.5 本章小结

本章主要介绍了 SNMP 协议的相关概念、结构和简单应用，并介绍了在操作系统中启用和配置 SNMP 服务。还介绍了 WMI 的概念、功能和简单应用。这些知识都是用好网络管理程序的基础知识。只有了解了基础知识，知道如何配置 SNMP 服务，才能真正将网络管理程序应用好。

第 5～8 章将重点介绍网络监测实用工具 IpSwitch WhatsUp Gold 的功能和应用。

第 2 篇　网络监测实战

第 5 章　WhatsUp Gold 安装和快速上手

对网络监测涉及的 SNMP 和 WMI 知识及其应用有所了解之后，从本章节起开始具体介绍监测工具的使用。首先介绍推荐的网络监测软件 WhatsUp Gold。本章主要介绍安装和快速上手的基础知识，包括两个部分：

- WhatsUp Gold 功能介绍及安装；
- WhatsUp Gold 程序的快速上手。

在快速上手部分，介绍 WhatsUp Gold 两个基础性功能，即查找网络设备和告警服务设置。其中简单介绍了通过 IP 段扫描设备方式添加简单声音告警提示的方法，让网管员对 WhatUp 功能有快速直观的了解，然后详细介绍该软件的功能和具体应用。

5.1　IpSwitch WhatsUp Gold 简介

IpSwitch WhatsUp Gold 提供快速反应、简洁易用的高效网络监控机制，全方位监测网络设备和应用程序，协助网络管理员实时掌控网络运行状态。WhatsUp Gold 能主动、全面发现网络设备及其关键服务，提供多种报警方式，因而能够避免因设备故障影响业务运作而带来的严重损失。WhatsUp Gold 使用全新的 Web 界面与技术，让网络管理员能够轻松控管网络设备与应用服务，维持网络的正常运行。

WhatsUp Gold 在网管软件市场中以其快速部署、操作容易、扩展性强、高性能等优势成长为网络设备及主机监控的领导品牌。目前，全球有超过 70 000 个网络在使用该软件。

5.1.1　WhatsUp Gold 功能综述

WhatsUp Gold 能够提供以下功能，帮助网络管理员有效管理网络。

- 网络管理。清晰地掌握网络系统结构，监控和管理包括路由器、交换机、服务器、打印机及其他网络设备，发现和跟踪网络中服务器的状态和性能，判断故障的发生，并在影响到终端用户之前迅速维修和恢复系统故障。
- 跟踪网络运行状态。发现故障则通过电子邮件、手机、短信、语音或系统工具等方

式发出报警提示和生成各种数据报表。

- 对系统资源的监测。通过 SNMP 或 WMI 方式监控 Windows 各类系统（Windows 2003、XP、Vista 和 Server 2008）和使用 SNMP 方式监控 Unix/Linux 系统，可监测操作系统几乎所有的资源，包括硬件、进程、服务、资源利用率（如 CPU、内存和磁盘的利用率）等，以了解系统及其业务的运行状态。
- 实现对解特殊设备性能的监测。例如，监测和采集空调温度、UPS 电压、打印机墨盒状态等参数。
- 应用程序监测。监测 IP 服务和协议，例如 Ping、TCP/IP、SNMP、WMI、FTP、Telnet、Exchange Services（SMTP、IMAP、POP3）、Web 服务（HTTP、HTTPS）、数据库服务、邮件系统等。
- 周期性搜寻网络设备，包括路由器、交换机、服务器、打印机及其他网络设备。能在数分钟内完成自动搜索服务，不断更新网络管理对象信息。

5.1.2 WhatsUp Gold 版本信息

WhatsUp Gold 提供了 4 个可用版本，分别介绍如下。

1．标准版本（WhatsUp Gold Standard Edition）

标准版本提供核心网络的管理特征，该版本是专为中小企业（SMB）设计的网络管理产品，让网络管理员专注于公司业务的监测，以确保企业关键应用系统的正常运作，如图 5-1 所示。

2．增强版本（WhatsUp Gold Premium Edition）

增强版本提供了标准版的全部监测功能，还增加了对 Exchange、SQL Server、SMTP Email 服务的监测，同时也支持使用 Microsoft WMI 方式的监测应用程序，如图 5-2 所示。



图 5-1　WhatsUp Gold 标准版



图 5-2　WhatsUp Gold 增强版

3．MSP 版本（WhatsUp Gold MSP Edition）

MSP 版本为托管服务供应商提供理想解决方案，供应商通过集中管理的网络控制中心，同时实现对多个公司不同网络的监测。该版本使用增强版本所有功能实现对网络的远程监控，如图 5-3 所示。

4．分布式版本（WhatsUp Gold Distributed Edition）

分布式版本是对增强版本的扩展，能够实现对跨越远程物理地址的广域网络实现统一监测和管理。该版本主要针对因物理位置分布广阔的大型企业，为企业提供容易部署、集中管理的解决方案，如图 5-4 所示。



图 5-3　WhatsUp Gold MSP 版本



图 5-4　WhatsUp Gold 分布式版本

由于 WhatsUp Gold Premium Edition 提供了对 Exchange、SQL Server、SMTP 等多种服务监测及通过 WMI 方式监测 Windows 操作系统，符合包含多种业务的中小企业网络管理者使用。本书以 WhatsUp Gold Premium Edition V11 版本作为讲解。

5.1.3　安装指南

1．软件的获取与系统要求

可通过 IpSwitch 的官方网站下载试用版本或通过代理商购买正版注册使用。

程序要求安装在 Windows XP Professional SP2 或更高版本，Windows 2000 SP4 Professional 或 Server 版本，或 Windows 2003 Server 系统中。浏览器要求 Microsoft Internet Explorer 6.0 及更高版本，或其他第三方浏览器。

2．程序安装

WhatsUp Gold V11 版本程序在安装完成后，所占空间约占 70MB。以下为安装步骤。

（1）双击安装程序进入安装界面，如图 5-5 所示。



图 5-5　开始安装程序

（2）安装程序进入数据库安装界面。WhatsUp Gold 程序支持 MSDE（Microsoft SQL Sever Desktop Engine 2000 桌面数据库引擎）和 Microsoft SQL Server 2000 数据库。安装程序已自带 MSDE 安装包，此处需要选择 MSDE 的安装文件路径和数据库文件路径，如图 5-6 所示。



图 5-6　选择 MSDE 数据库安装目录

选择 MSDE 安装路径后进入 MSDE 的安装，如图 5-7 所示。

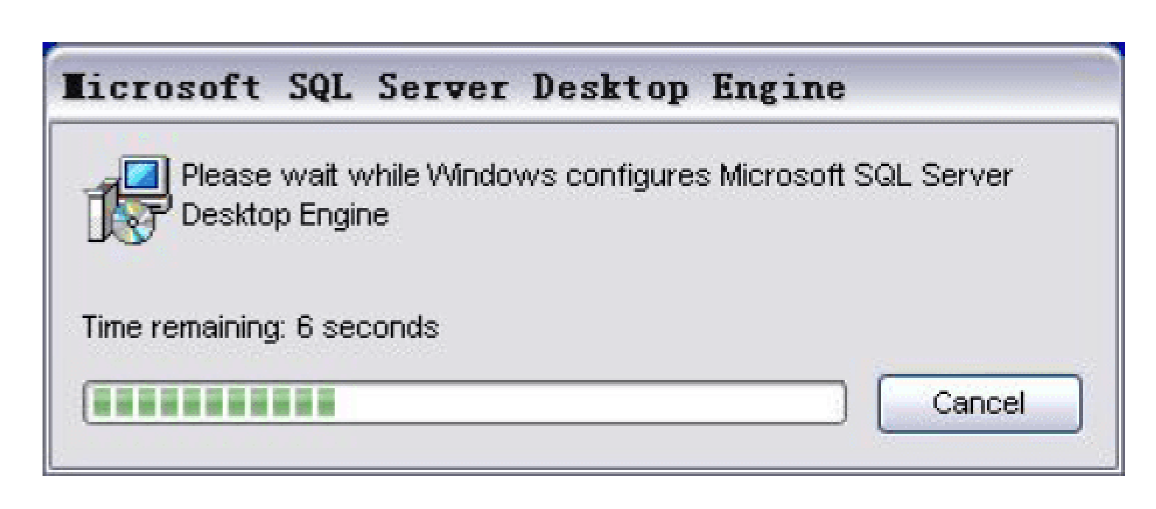


图 5-7　开始安装 MSDE

（3）如果系统中已经安装过 MSDE，那么安装程序会提示是否需要备份现有数据库。如需备份，可选择将数据库备份的指定目录。首次安装 WhatsUp Gold 不会提示该选项，

如图 5-8 所示。

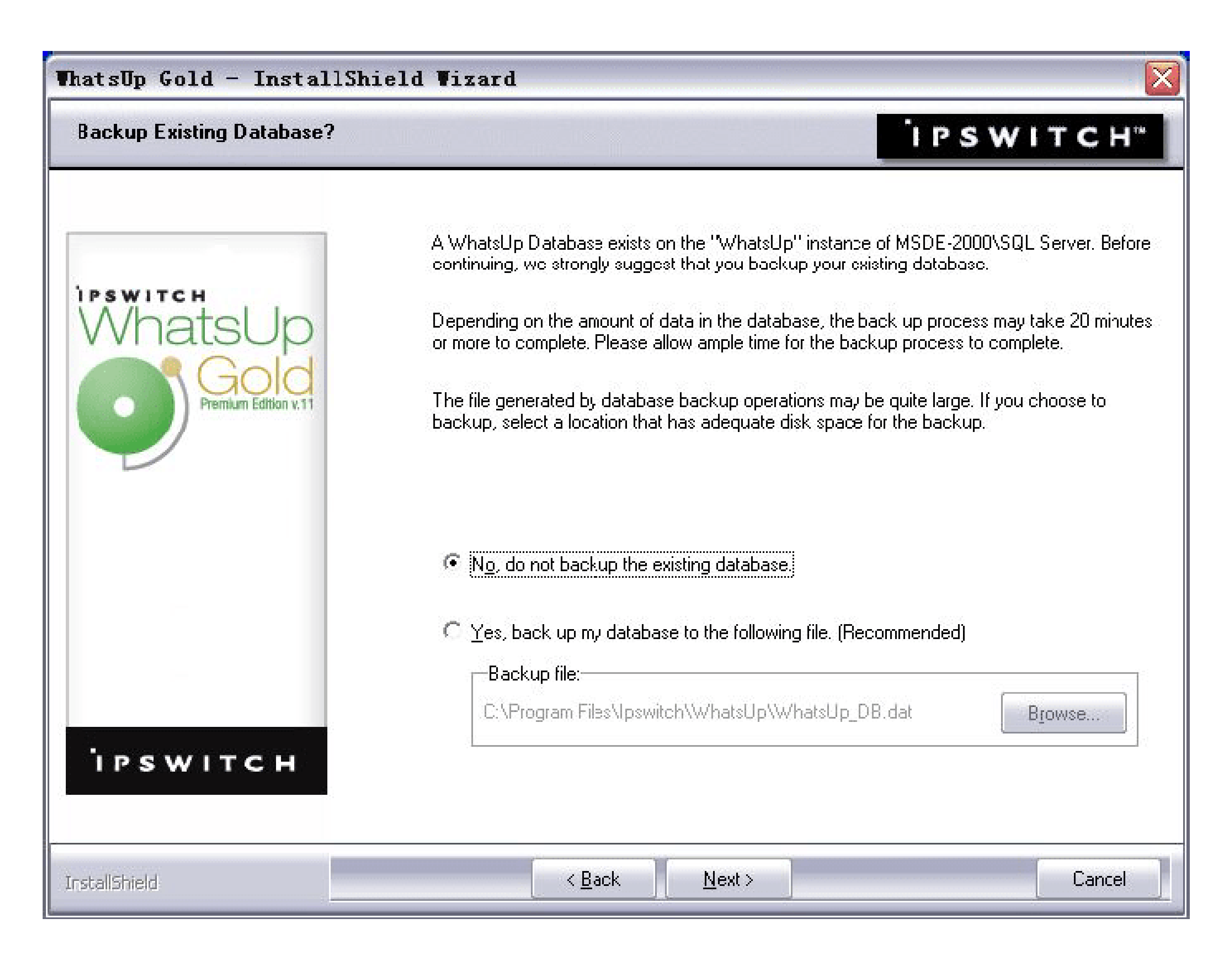


图 5-8 选择是否备份当前数据库内容

（4）安装 MSDE 完毕后进入 WhatsUp 主程序安装界面，首先选择程序安装目录，如图 5-9 所示。



图 5-9 选择安装目录

（5）选择下一步后，程序询问“是否允许 Web 页面服务模式并自动设置 Windows 防火墙允许（默认推荐）”，Web 服务器使用的默认端口为 80，如果该端口已经被其他程序占用，那么可以为其设置其他端口编号，此处采用默认选项，如图 5-10 所示。

（6）选择下一步后，程序即完成设置并开始安装。安装完毕后，需要对程序进行注册，可通过购买正版许可获取注册码。

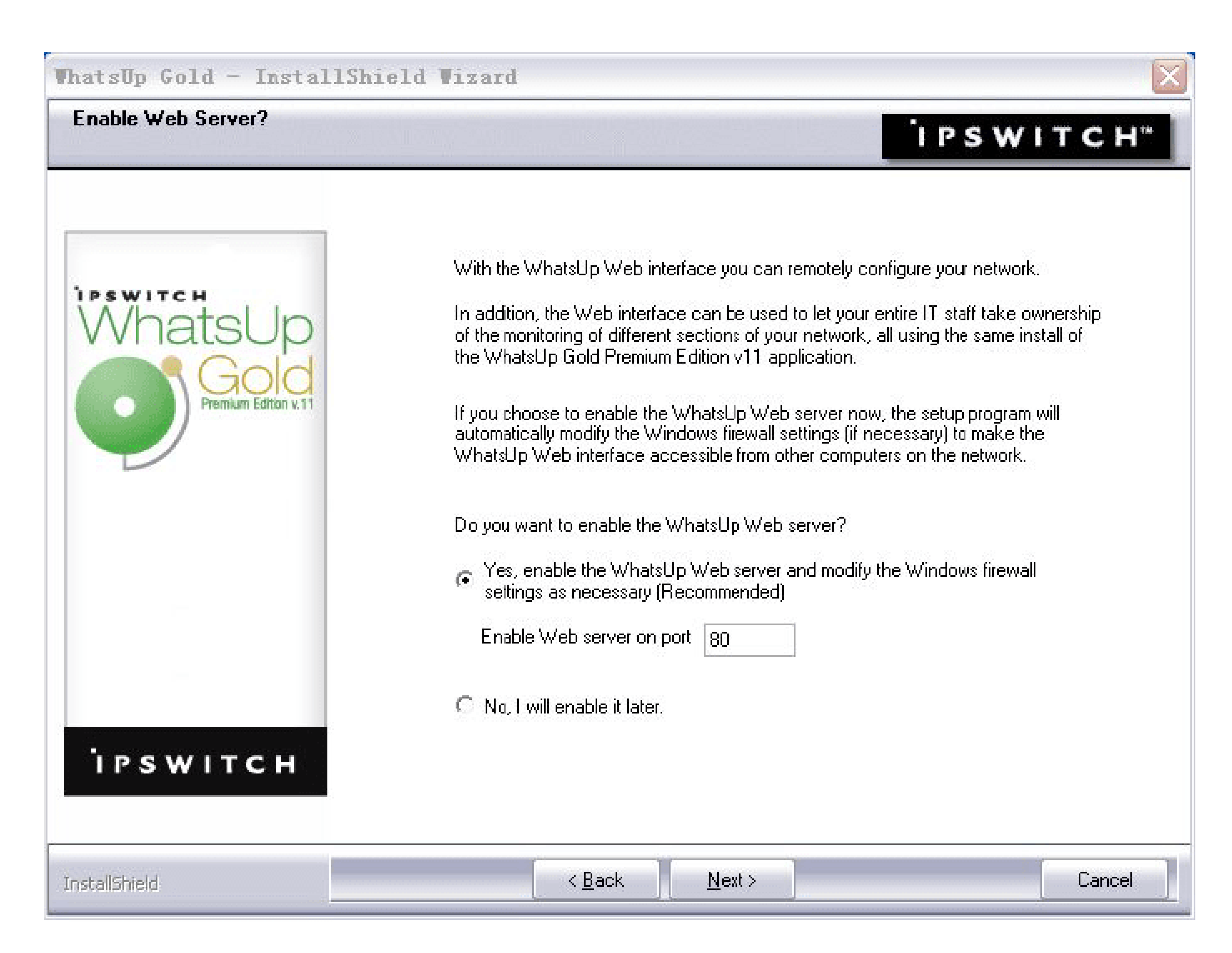


图 5-10　设置 Web 服务器使用端口

安装正常结束后，WhatsUp Gold 会在屏幕右下角生成任务托盘图标。该图标在运行期间，作为整个监控程序运行状态的报警提示。该图标显示的是所有设备状态中最严重的故障状态。此外，该托盘程序对系统中设备状态的改变弹出提示信息框。

以下为 3 种系统状态的图标，绿色标识所有设备正常，黄色为系统存在一般性告警（例如 SSH 无法登录），红色为严重告警（例如设备无法 Ping 通等），如图 5-11 所示依次为绿色、黄色和红色。

图 5-11　WhatsUp Gold 托盘图标状态

当发现 WhatsUp Gold 轮询服务引擎为停止状态时，托盘图标会显示图案，在这种情况下，WhatsUp Gold 无法连接数据库。各项服务及设备状态都无法正常运行。此时，需要重新启动 WhatsUp Gold 服务进程。

WhatsUp Gold 安装完成并正常启动后，在【控制面板】|【管理工具】|【服务】里，将看到共有 3 项服务进程，分别是 WhatsUp GoldWeb 服务、轮询服务引擎和链接 MSDE 数据库服务。如果 WhatsUp Gold 程序运行出现异常，可检查这 3 项服务是否正常启动，如图 5-12 所示。



图 5-12　WhatsUp Gold 程序服务进程

5.1.4　卸载 WhatsUp Gold 程序

卸载 WhatsUp Gold 操作步骤如下：

（1）在 Windows 系统控制面板中，打开【添加或删除程序】对话框，找到要卸载的 WhatsUp Gold 项，选择卸载即开始删除程序。删除程序首先会提示，删除 WhatsUp 主程

序但保留采集到的网络数据，或者删除程序和所有数据，如图 5-13 所示。

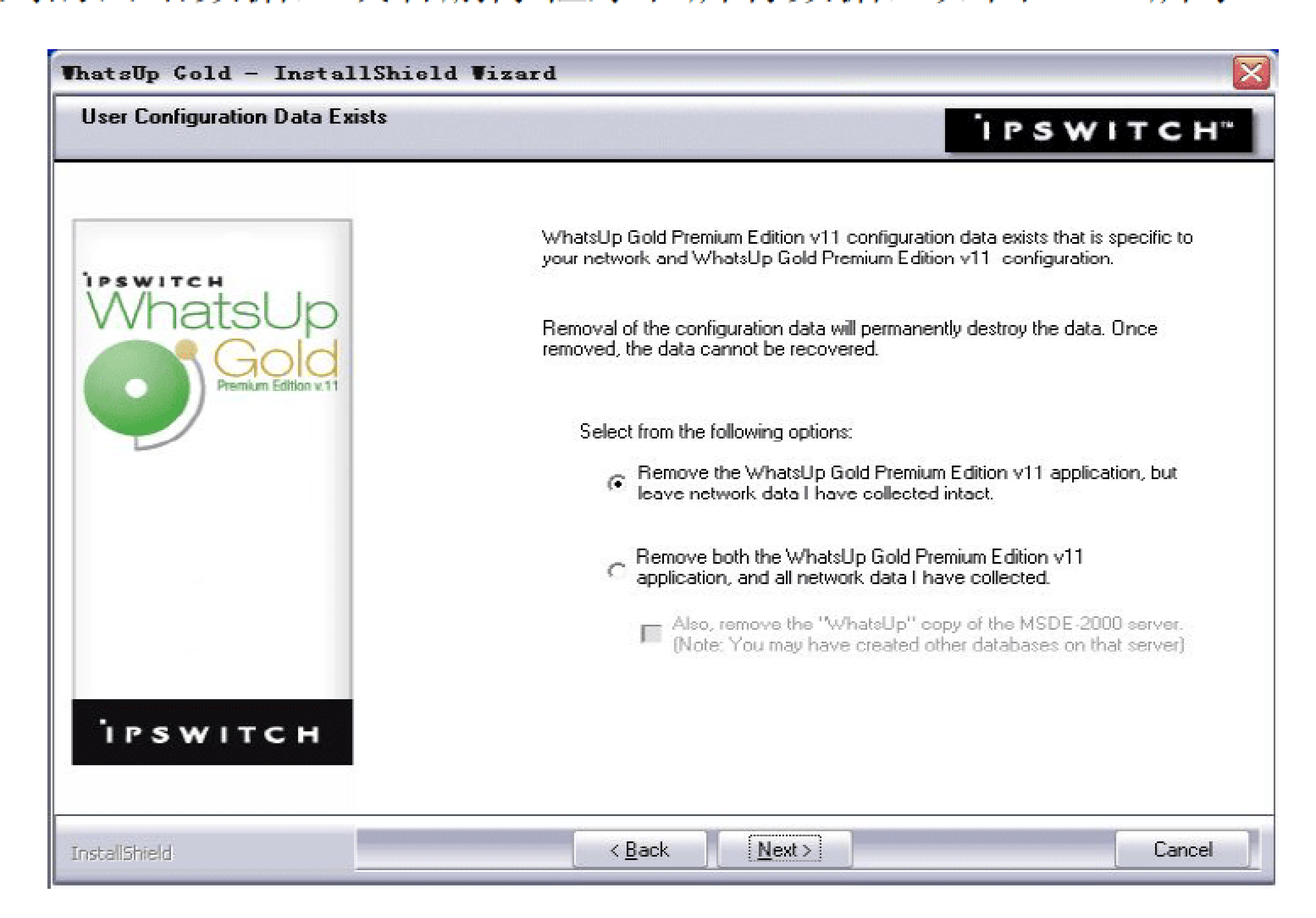


图 5-13　选择卸载程序是否保留数据

（2）卸载完成后提示是否立即重启电脑，如图 5-14 所示。

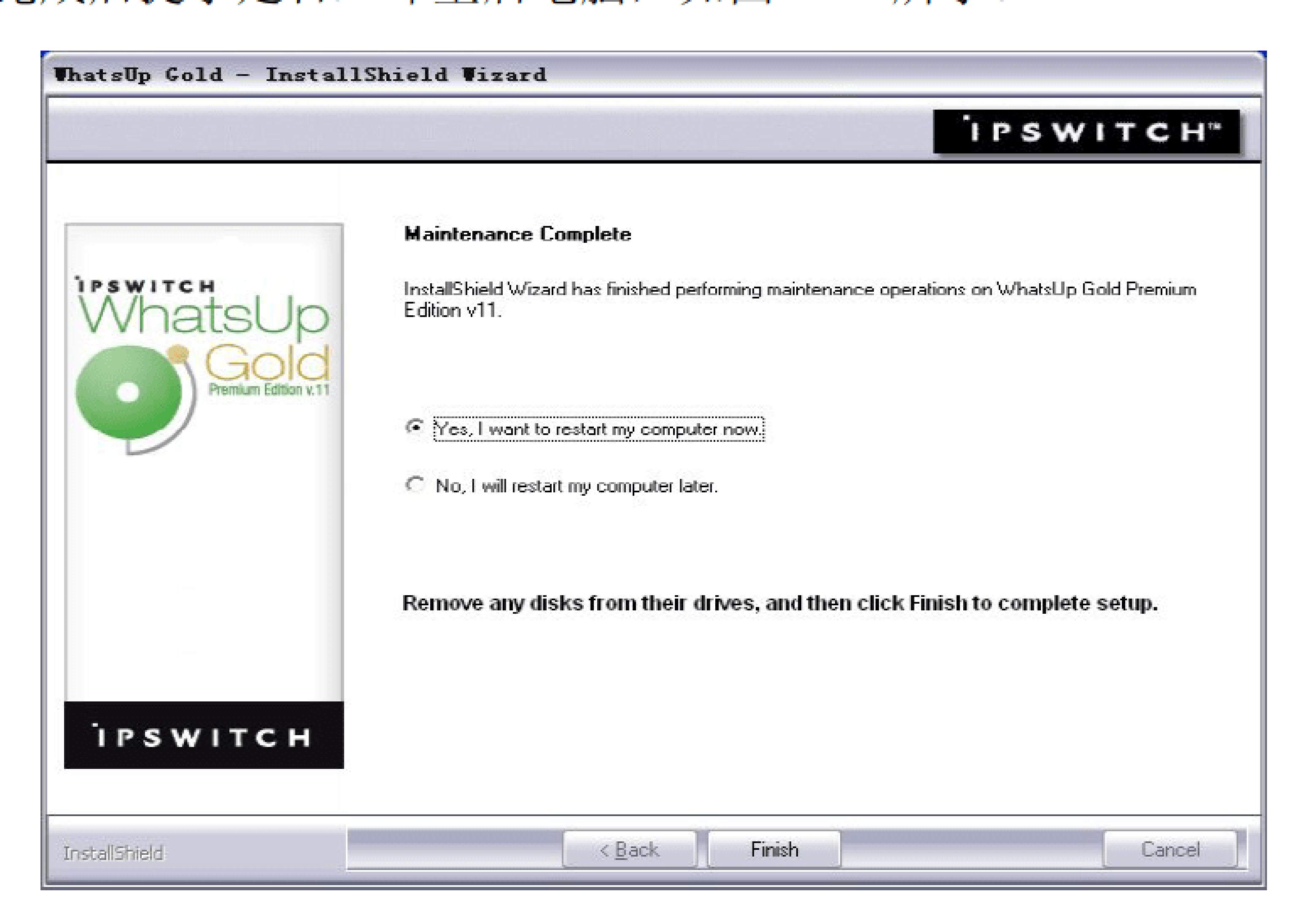


图 5-14　WhatsUp 主程序卸载完毕

（3）卸载 WhatsUp 主程序后，还可以选择是否卸载 MSDE 数据库。如需要卸载，找到 MSDE 项直接卸载即可，如图 5-15 所示。

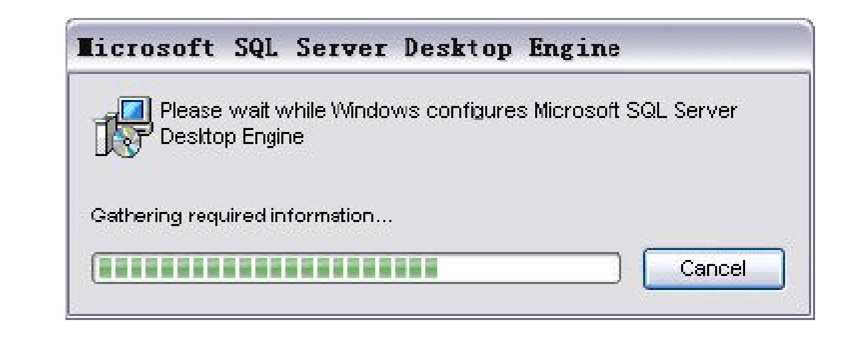


图 5-15　卸载 MSDE 数据库

5.1.5　数据库备份和还原

可以通过 WhatsUp Gold 中的数据库工具来备份和还原数据库。在主界面中，选择菜单命令 Tools | Database Utilities | Backup SQL Database 即可备份数据库文件。只需选择库

文件的备份目录，库文件存储为.dat 格式的文件，如图 5-16 所示。

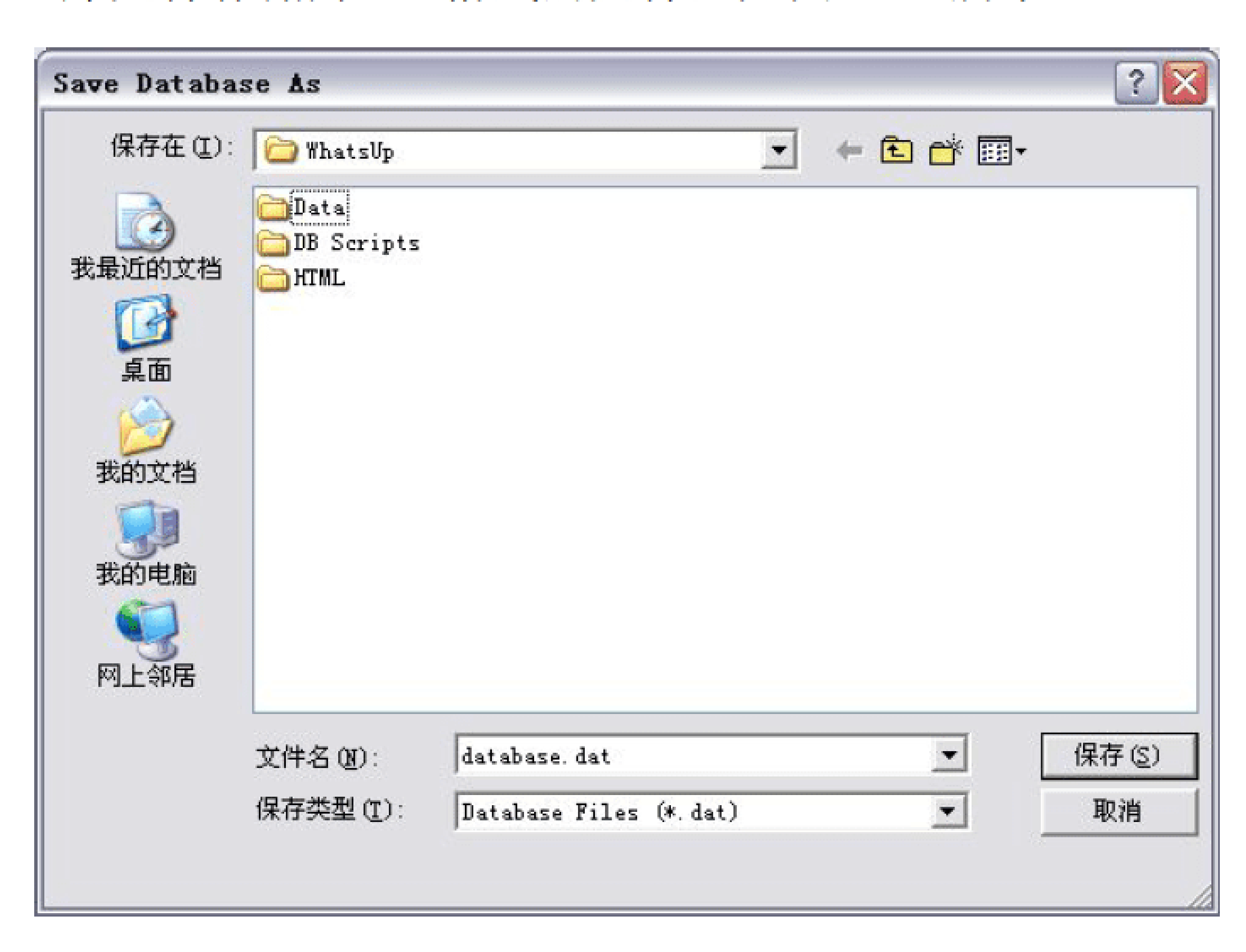


图 5-16　备份数据库文件

还原文件时，执行 Tools | Database Utilities | Restore SQL Database 命令，并选择需要还原的.dat 文件后，将覆盖现有的 WhatUp Gold 数据库。

5.1.6　数据库辅助工具的使用

数据库辅助工具发现和定位数据库故障，用于监视数据库容量大小和优化库表中索引碎片比例。过多的索引碎片会造成 SQL Server 中的 Index Page（索引页面）占用比实际所需大得多的存储空间。那么在查询过程中按索引扫描数据时，增加了 Logical READS（内存在读取的数据块）、I/O 等操作，从而影响数据库的性能。

碎片比例过高导致数据库运行效率降低，类似于计算机磁盘中碎片过多影响计算机运行速度。使用该数据库工具能够管理数据库索引碎片及清理过期无用数据。在 WhatsUp Gold 主界面中，选择 Tool | Database utilities | Tools 命令，进入数据库维护界面，如图 5-17 所示。

该界面提供了两项功能：Performance（性能管理）和 Table Maintenance（表维护管理）。分别介绍如下。

Performance：扫描和优化数据库。在 Performance 页面中，单击 Check for fragmented tables 按钮，执行数据库表扫描。扫描结果将列出索引碎片比例超过 10%的库表。然后选择需要优化的库表，并单击 Optimize selected tables 按钮执行优化表操作，WhatsUp 将自动停止服务并优化数据表，优化结束后自动重启服务，如图 5-18 所示。

同时，在界面的下方列出了数据库当前容量大小及所占最大可用空间（默认 2GB）的比例。单击 Validate and compact database 按钮，则将执行对数据表、索引、数据库连接的验证和压缩存储数据表，释放更多空间。WhatsUp Gold 在执行完该操作同样会自动停止和重启服务。

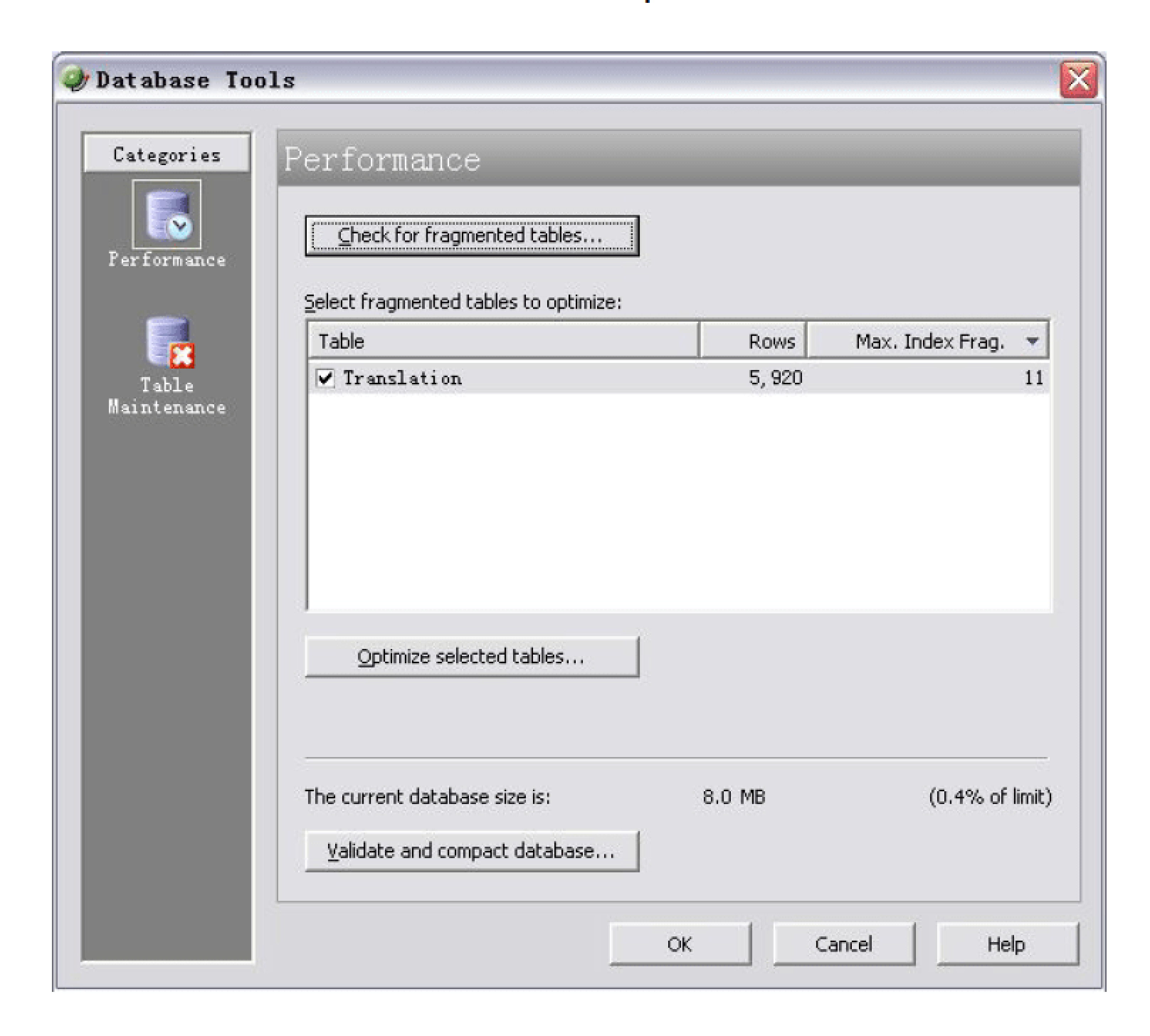


图 5-17　数据库维护界面

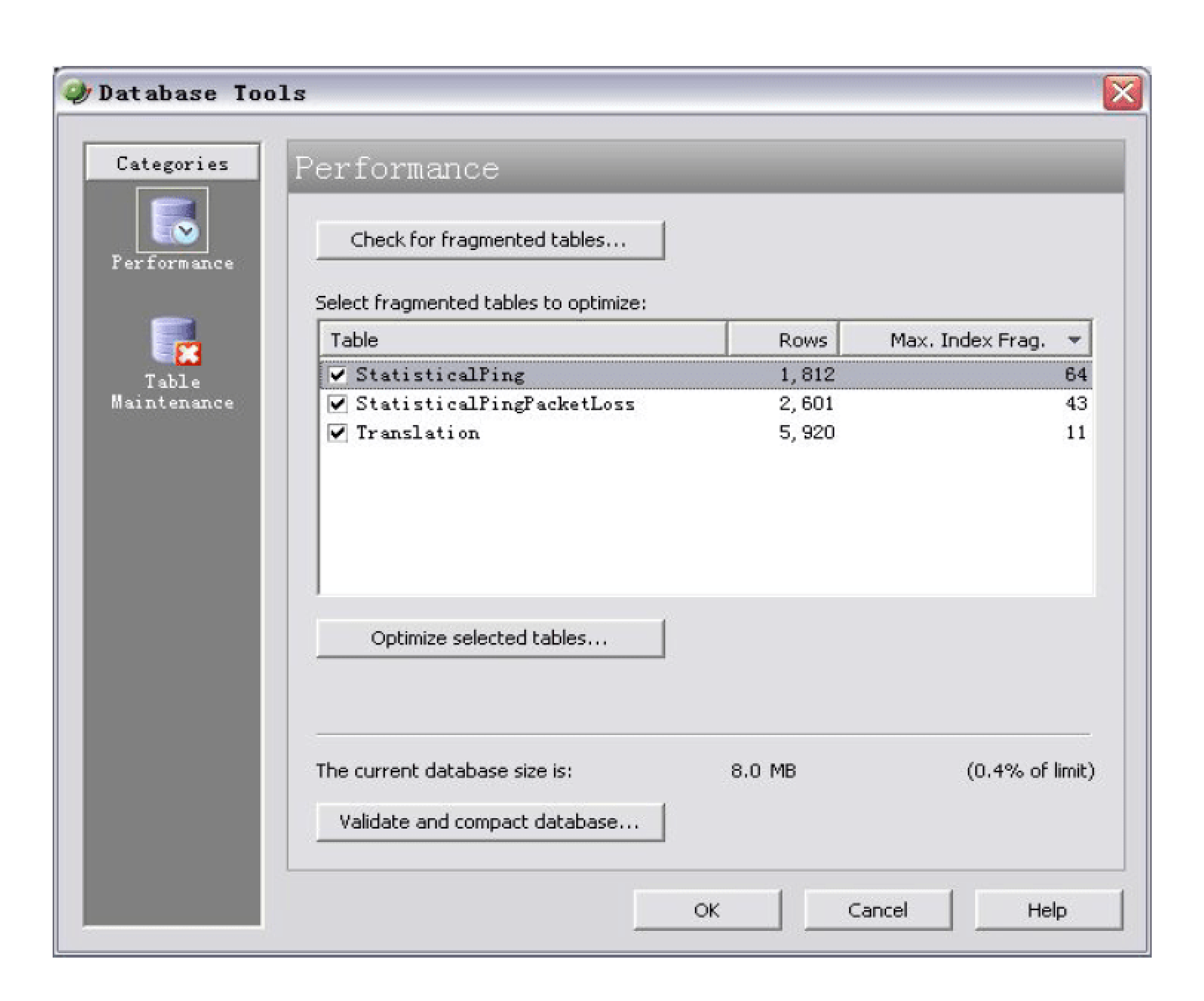


图 5-18　优化数据库

Table Maintenance：清除过期无效的表数据。在 Table Maintenance 页面中，列出了 3 类可做清理的数据库表，用于主动监控程序的数据表、报表数据表和其他数据表。在表格中列出了每一类表的总行数 Total Rows 及过期数据行数 Expired Rows。单击 Purge Expired Rows 按钮，开始执行无效数据的自动清除操作，如图 5-19 所示。

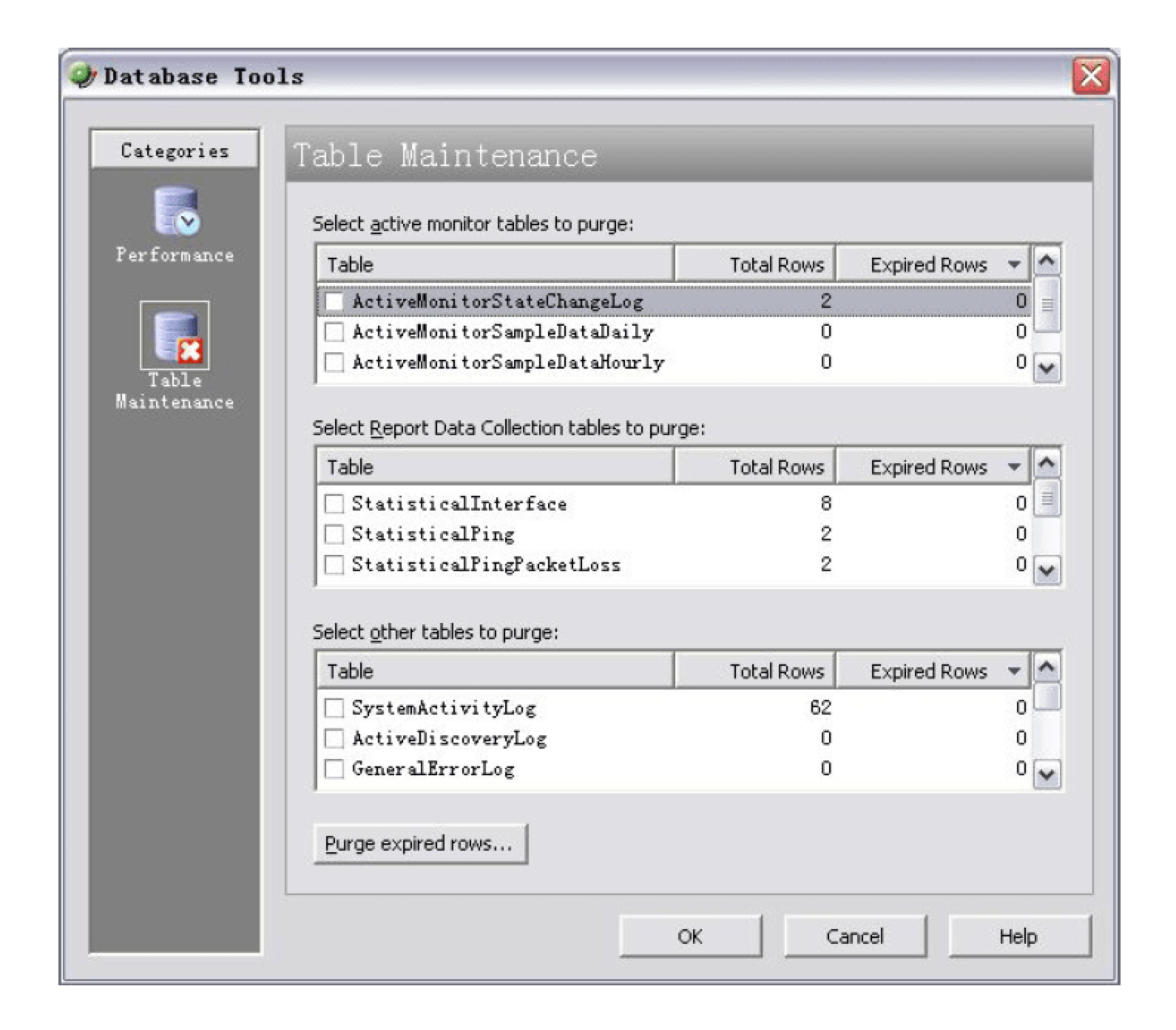


图 5-19　清除无效的数据

注意：执行该操作清除的数据将无法恢复，建议执行操作之前备份数据库文件。

5.2 WhatsUp Gold 快速入门

在对 WhatsUp Gold 概念及功能有个初步了解后，本节对 WhatsUp Gold 的主界面、扫描发现网络设备及 Web 视图内容进行简单介绍。

5.2.1 WhatsUp Gold 控制台界面介绍

WhatsUp Gold 具备简洁和易懂的操作界面，能够对网络所有设备及状态一目了然。其主界面的主要功能区域如图 5-20 所示。

在图 5-20 中，标注了 8 个功能区域，图中的序号和下面的序号对应介绍如下。

1．Web 视图界面：WhatsUp GOld 提供了控制台和 Web 页面两种控制界面，单击图标，即可进入 Web 页面视图。在 Web 视图中，提供了设备管理和各类报表信息。

2．设备组树 Device Group：通过树形结构展示了网络设备组，每次执行扫描操作都会在该树顶级目录下增加一个设备组，设备组中包含当次扫描的所有设备。在设备树中，能够对各组设备执行拖放、更名、增加、删除等操作。

3．设备列表：该窗口显示对应设备组中的所有设备，可根据需要对设备修改显示名、删除、Ping、增加设备等操作。

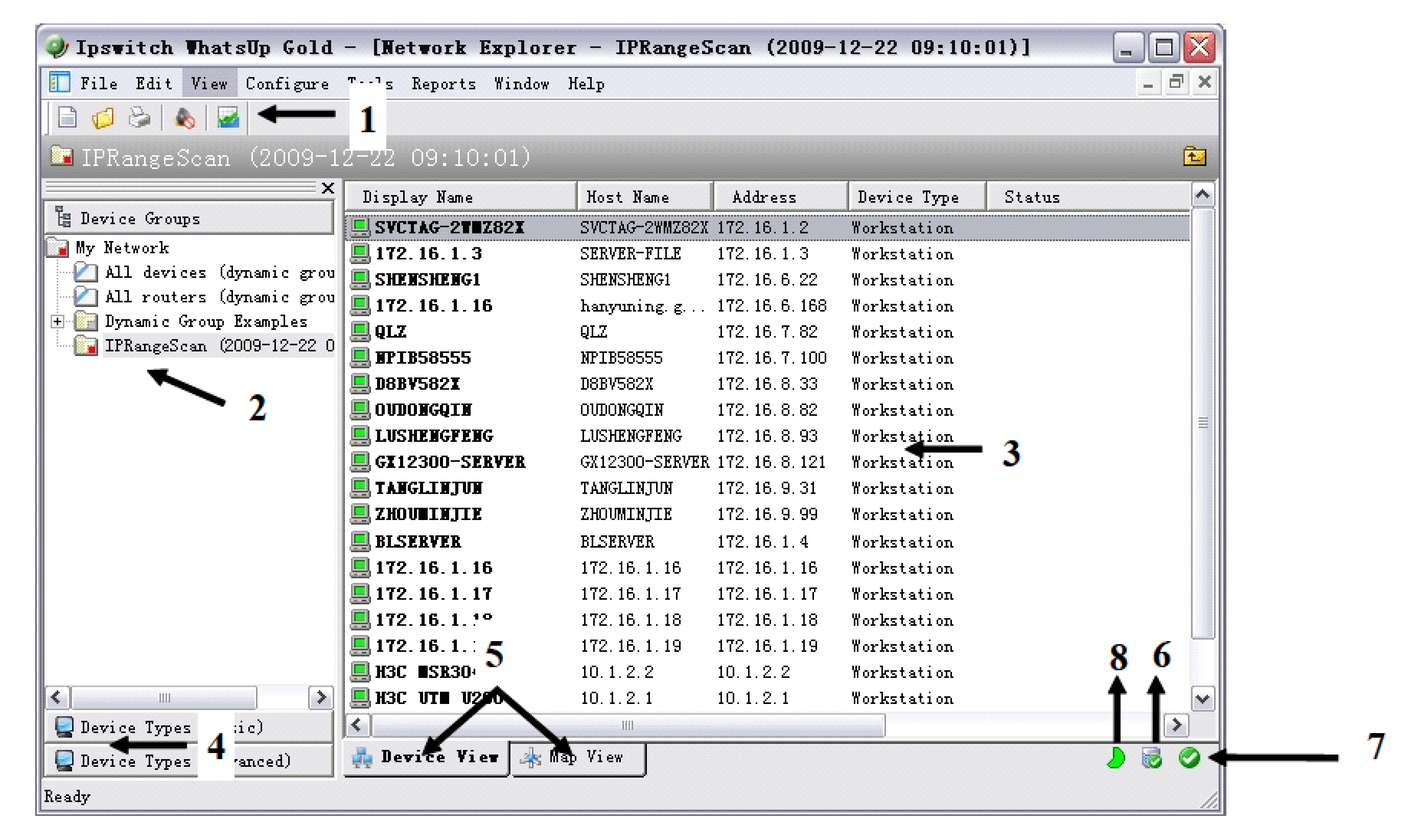


图 5-20 主界面功能区域

4．设备类型：基础或高级设备图标面板，列出了能够添加到 WhatsUp 中的设备类型图标，其中包括服务器、工作站、网络设备及打印机等，可直接拖放到主界面窗口中进行设备的添加。

5．设备拓扑图显示模式：在 Device View 模式中，主窗口中以列表方式显示对应设备组的全部设备图标；在 Map View 拓扑图模式中，可根据网络结构调整设备的位置和添加设备连线，以及更名、删除等操作。Map View 视图如图 5-21 所示。

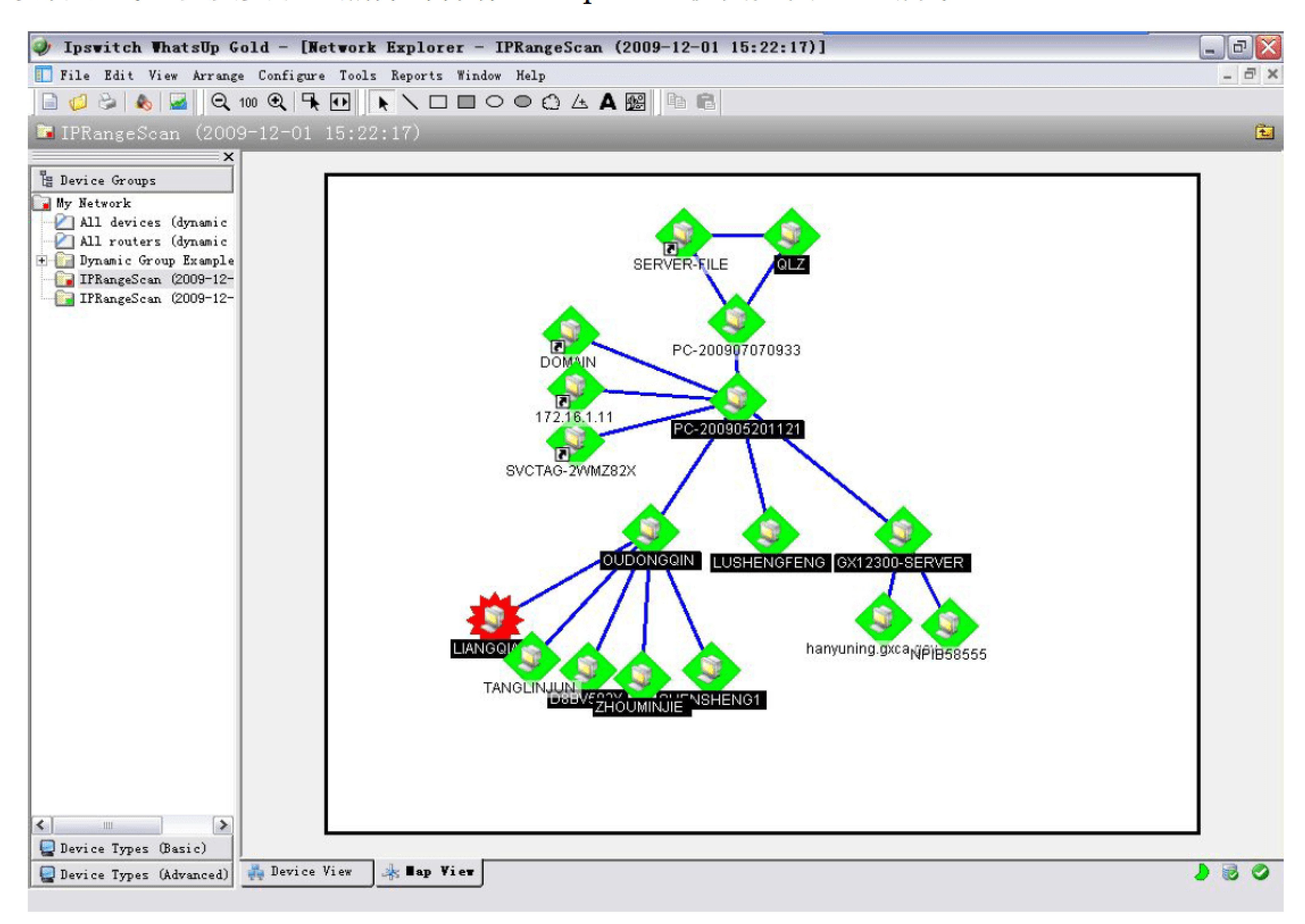


图 5-21 WhatsUp Gold 拓扑图视图

6．轮询操作引擎：WhatsUp 采用定期检查设备状态的轮询机制，单击该图标可查看轮询操作引擎是否运行正常。如果运行正常，将提示控制台与轮询操作引擎连接正常；如果连接不正常，则图标显示为。

7．轮询状态：是否已启动轮询机制，该图标表示轮询服务启动正常。如果未启动，则图标显示为。

8．数据库容量：鼠标悬停该图标时，将提示当前数据库使用量，使用容量超过 50%时，该图标显示为黄色。

5.2.2 扫描发现网络设备

使用设备扫描向导发现网络设备，包括 4 种扫描方式。首先介绍作为快速入门的 IP 地址段扫描模式，即按照提供的 IP 段范围逐个扫描目标地址发现设备，并为扫描到的设备添加连通性的轮询监测。操作步骤如下：

（1）在主界面中，选择主菜单的 File | Discover Devices 命令，打开设备发现向导窗口，并选择 IP 区间扫描模式，如图 5-22 所示。

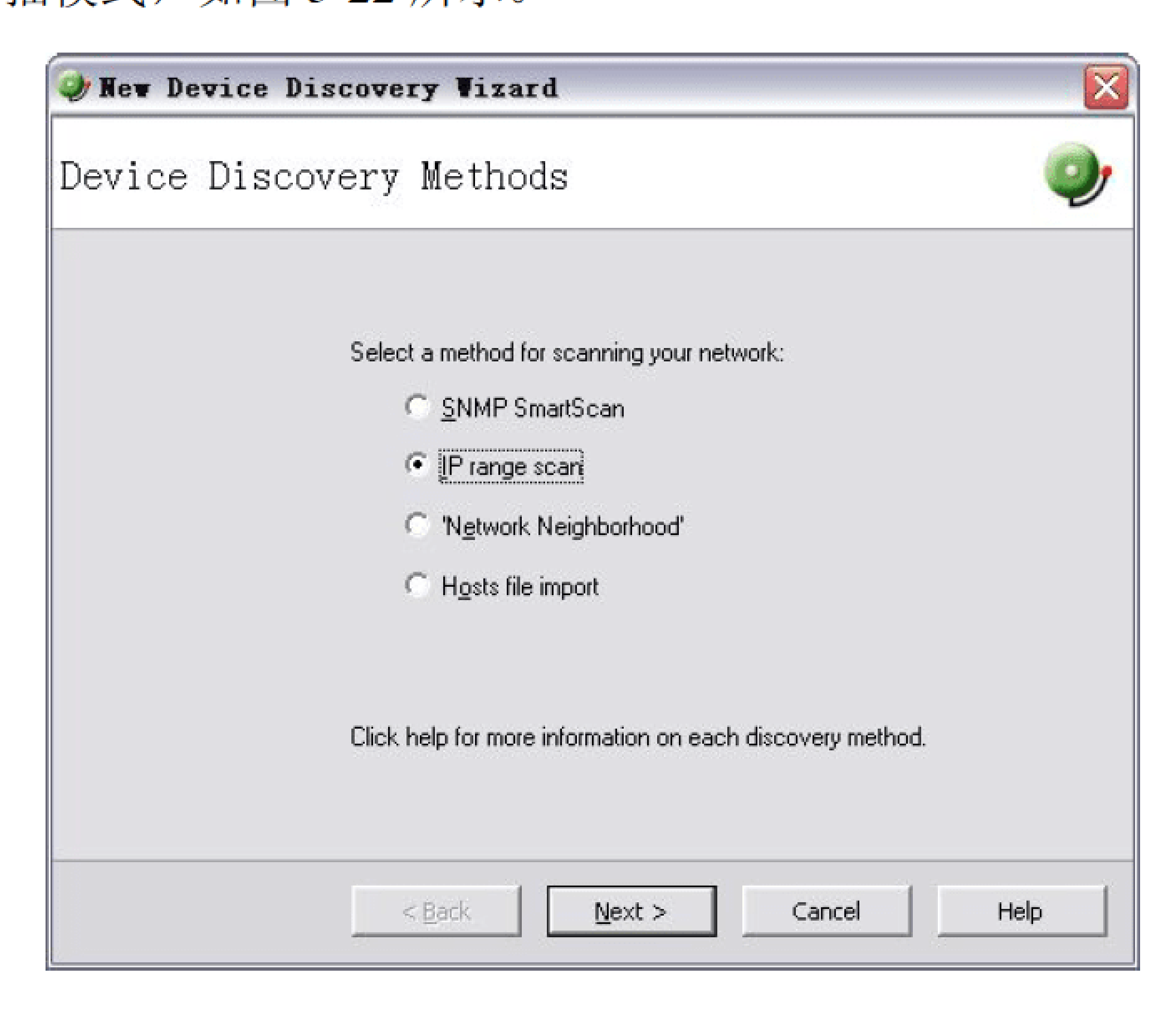


图 5-22 设备扫描向导

（2）选择 IP 段扫描模式后，输入起始 IP 地址和结束 IP 地址，本例为 172.16.1.1～172.16.6.254。IP 段的设置可根据网络实际情况进行设置，WhatsUp Gold 将逐台扫描 IP 段内的所有地址，如图 5-23 所示。

（3）单击 Next 按钮进入社区字符串的设置界面。由于目前仅添加设备联通性的监测，所以并不用通过 SNMP 方式或 WMI 方式采集更多的属性。在 SNMP read community 输入框中可不填写内容或输入默认的 public，在 Windows credentials 选择框中选择 None，如图 5-24 所示。

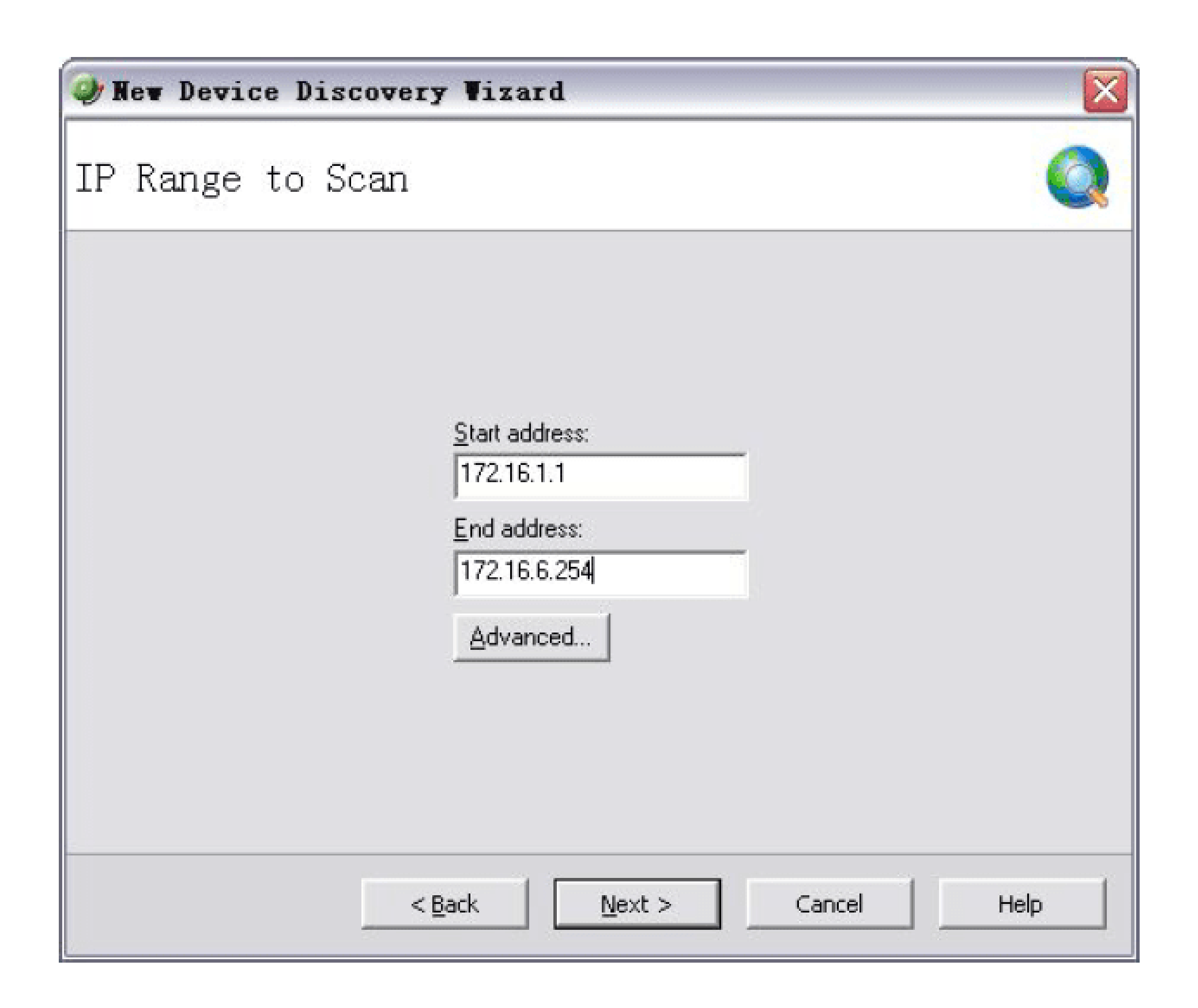


图 5-23　输入扫描的 IP 范围

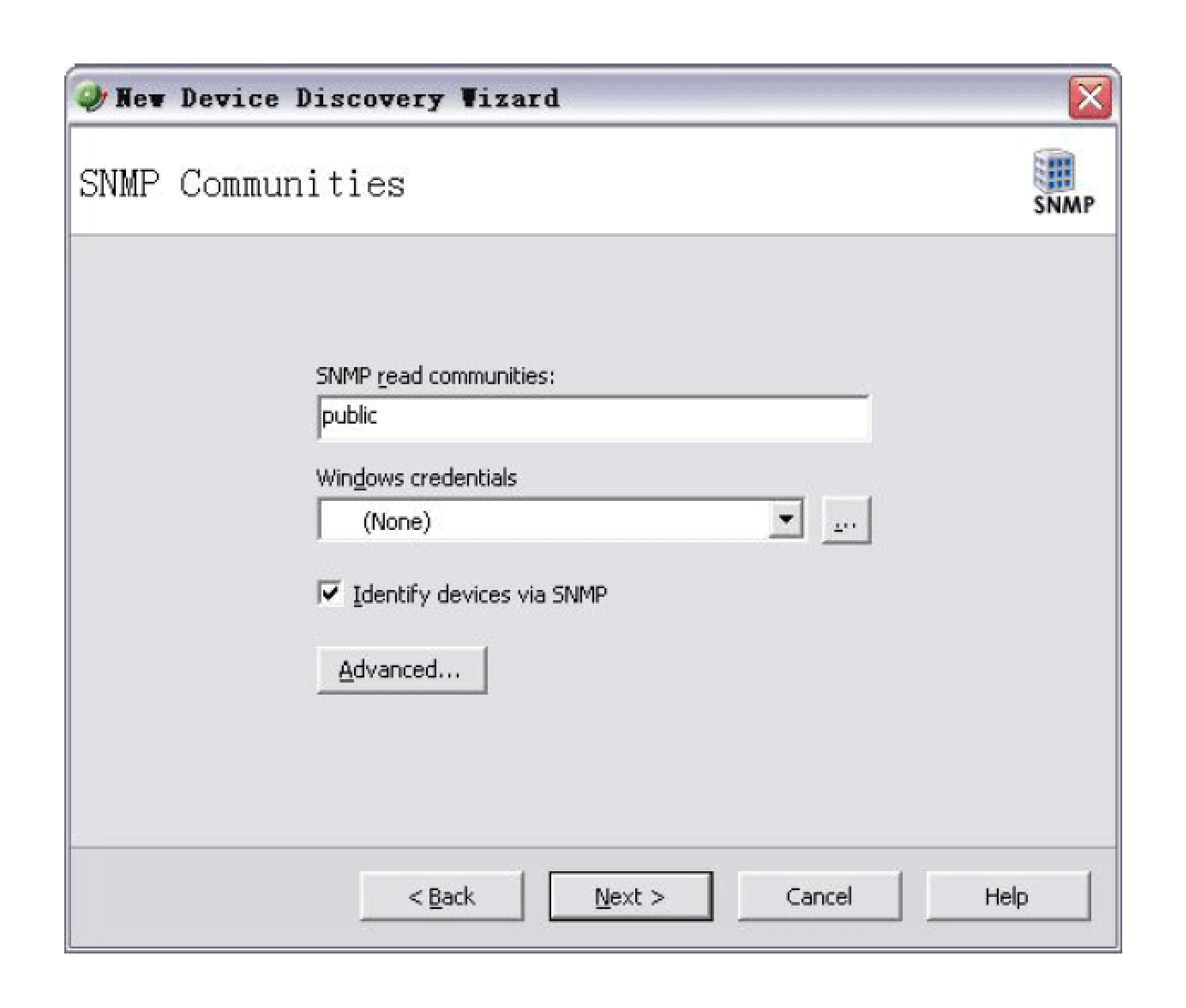


图 5-24　添加 SNMP 安全认证字符串设置

（4）单击 Next 按钮进入监控对象选择界面，此处仅为该组设备添加是否能 Ping 通的监测，以及 Ping 操作延时和可用性。在 Active Monitors（主动监测对象）中选择 Ping，并选择下方的 Ping Latency and Availability 选项，如图 5-25 所示。

（5）单击 Next 按钮进入下一步，开始执行扫描操作，如图 5-26 所示。

（6）执行完 IP 段扫描后，将发现网络中可连接的设备列表（如图 5-27 所示）。本次扫描操作共发现 7 台设备。本次扫描操作将生成一个设备组。

（7）单击 Next 按钮将进入报警提示动作的设置界面。当设备状态变化时触发报警提示动作。由于初次使用 WhatsUp Gold，所以尚未建立报警提示动作。此处先选择不执行任何报警提示动作。自定义配置提示动作将在第 6 章中详细介绍。报警设置如图 5-28 所示。

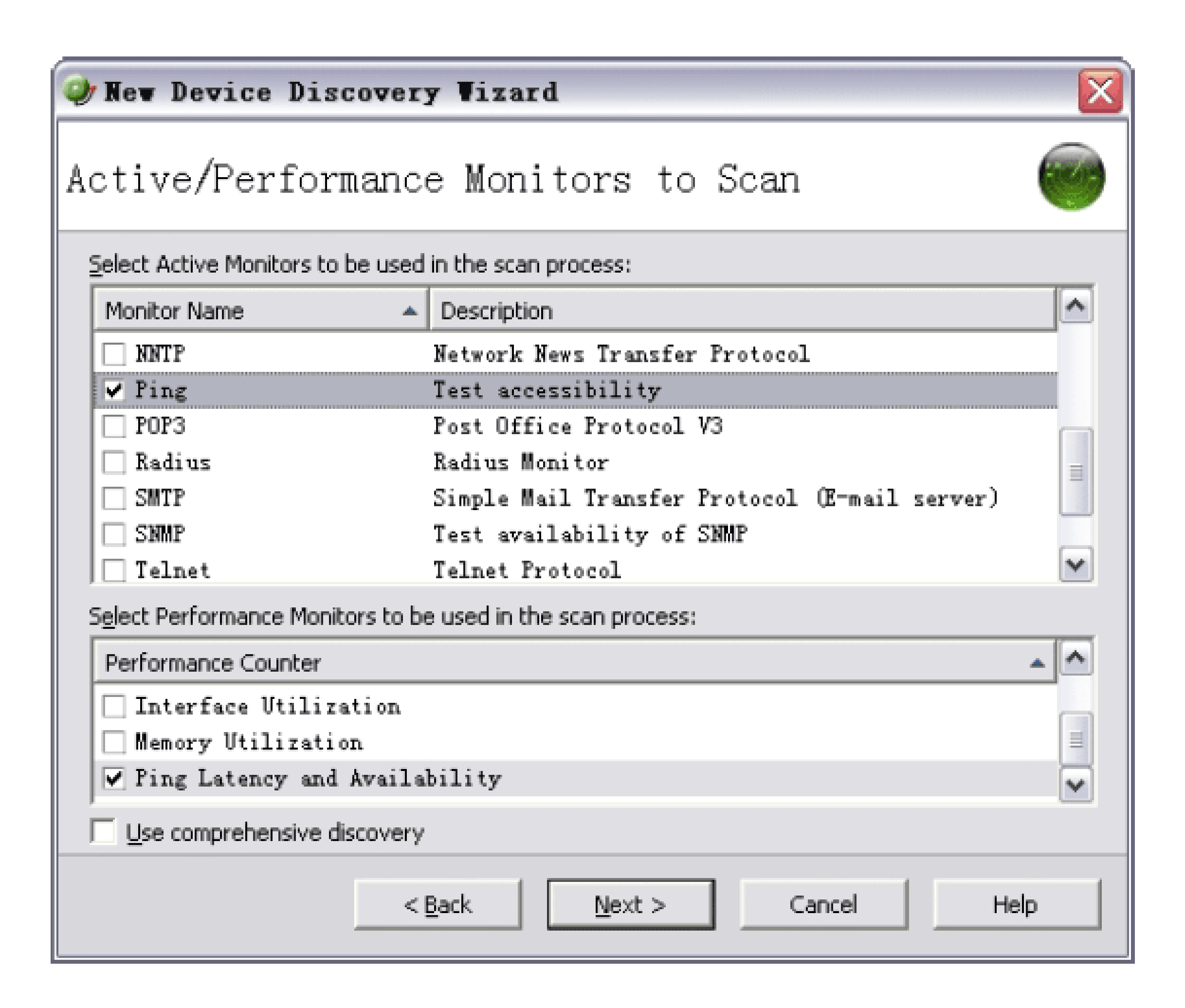


图 5-25　为设备选择添加监测对象

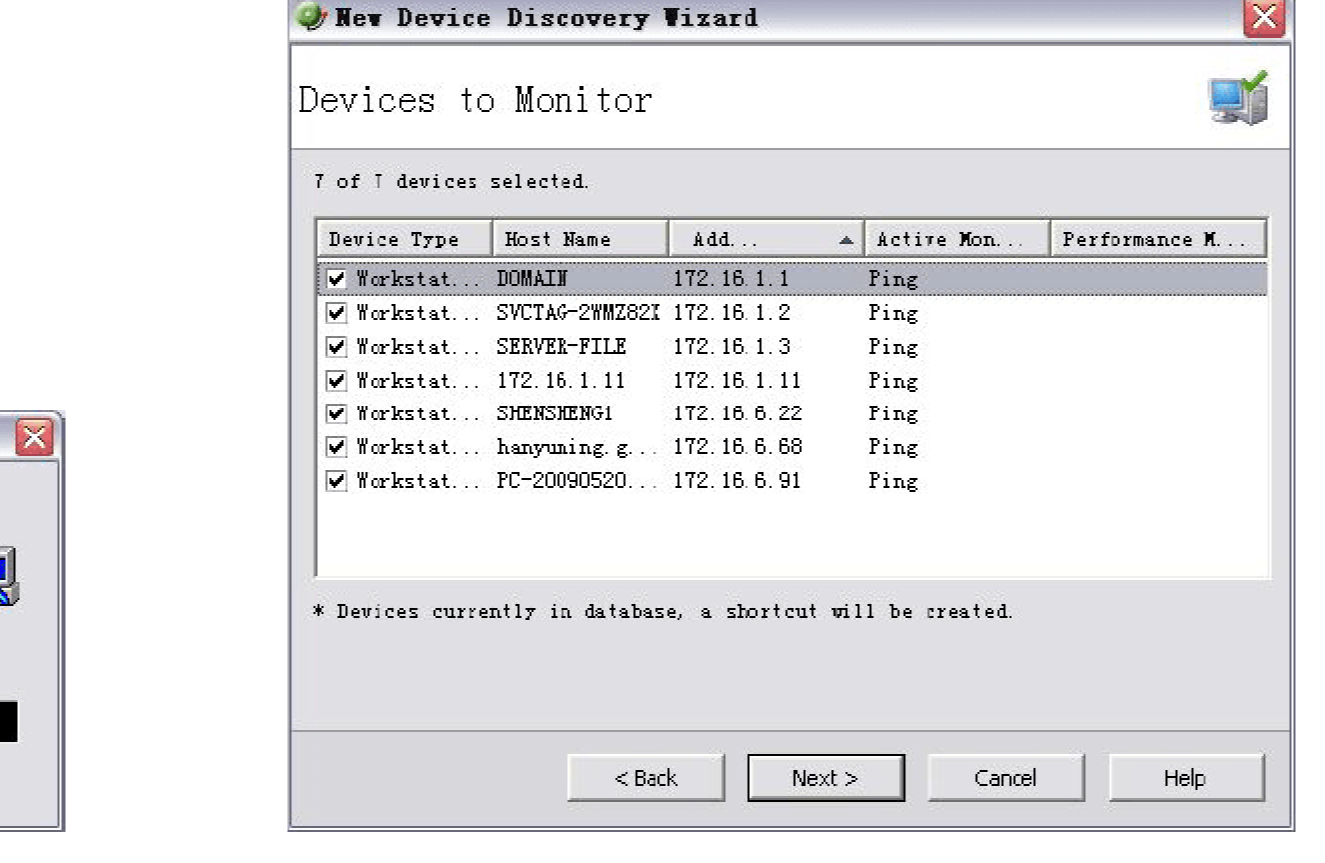


图 5-26　扫描网络设备

图 5-27　扫描完成发现网络设备列表

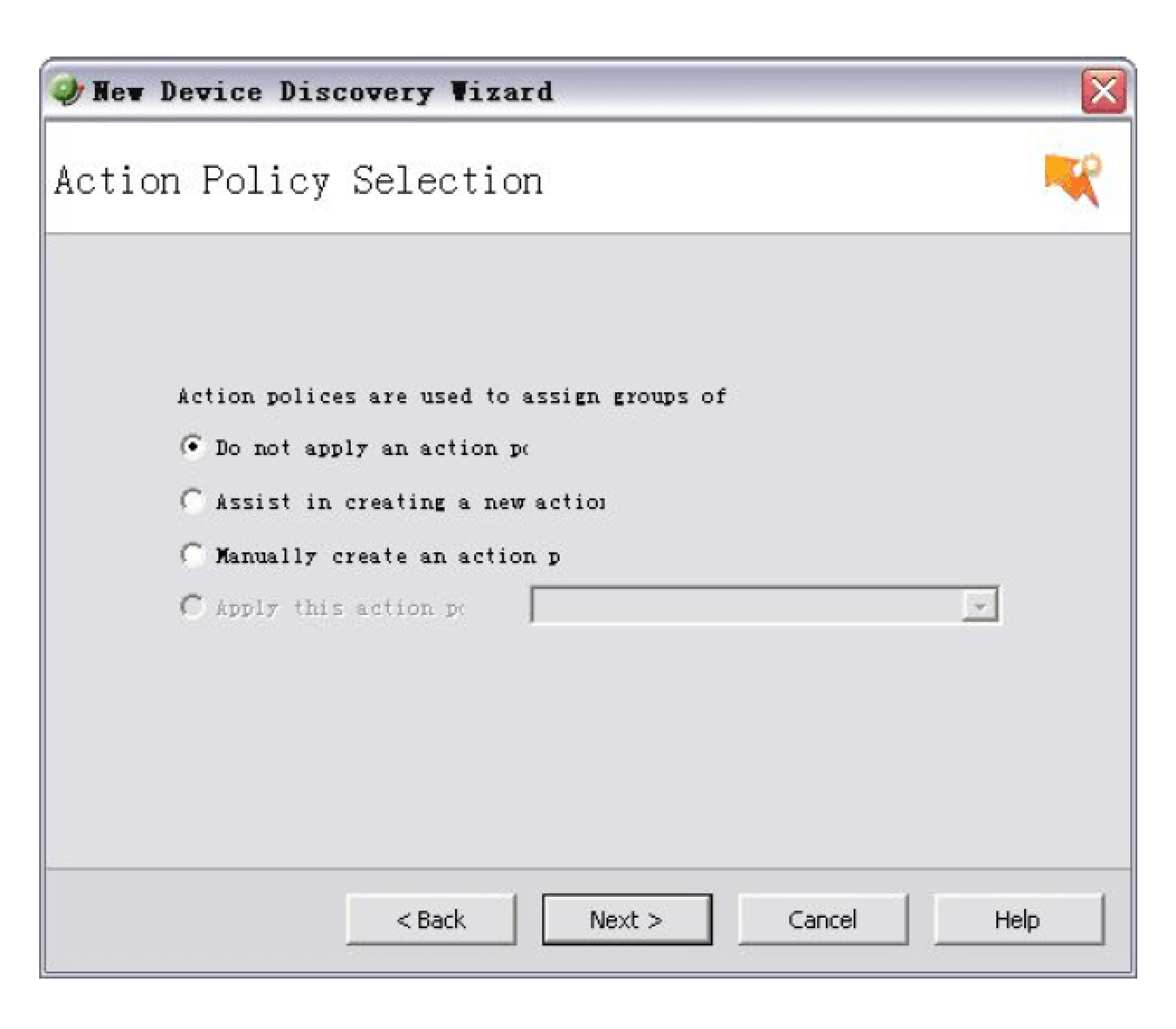


图 5-28　选择不执行任何报警提示动作

（8）单击 Next 按钮进入下一步后将完成本次扫描操作，WhatsUp Gold 将在主界面设备列表窗口中添加搜索到的设备列表，如图 5-29 所示。

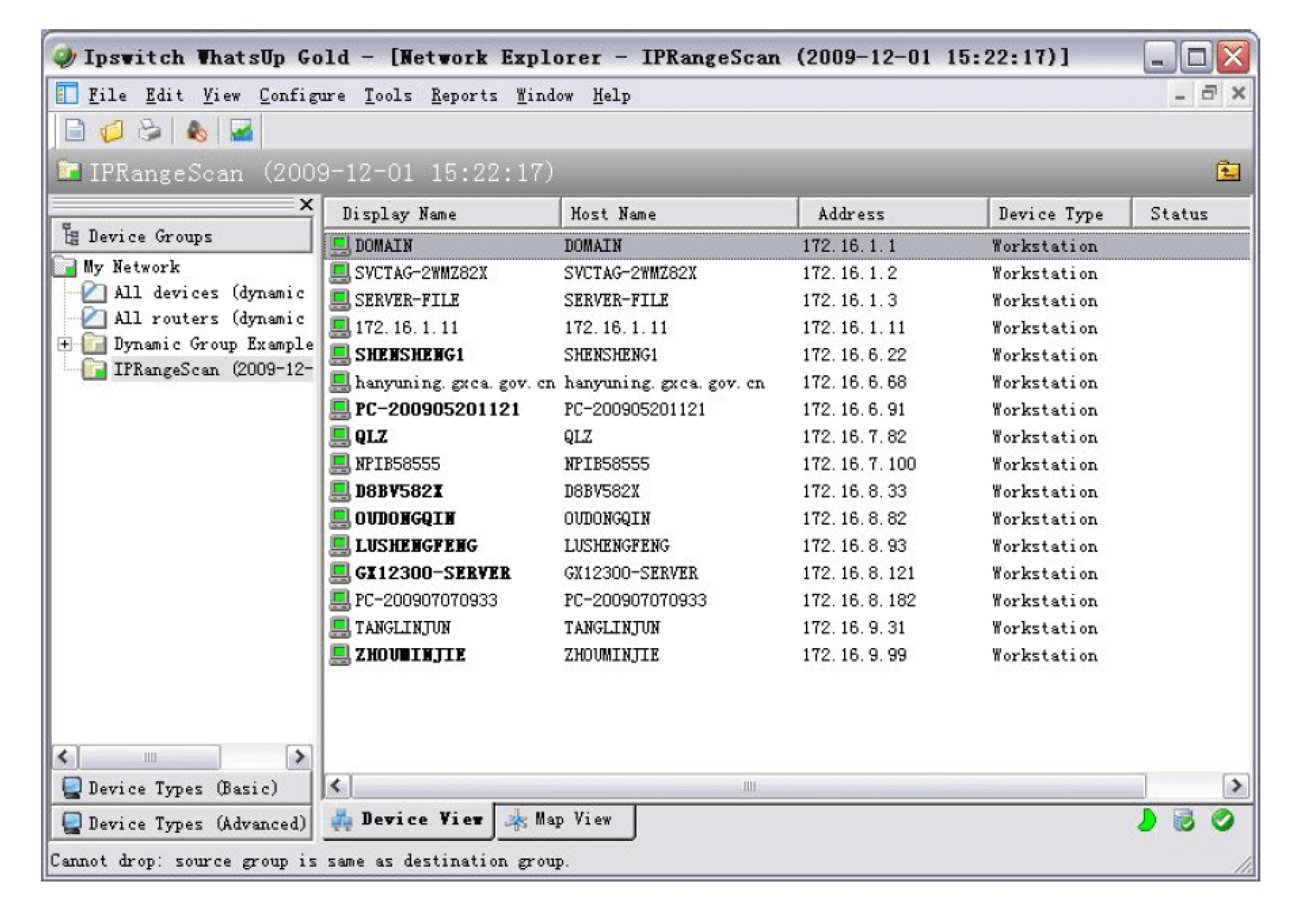


图 5-29　扫描完成在主界面中生成设备列表

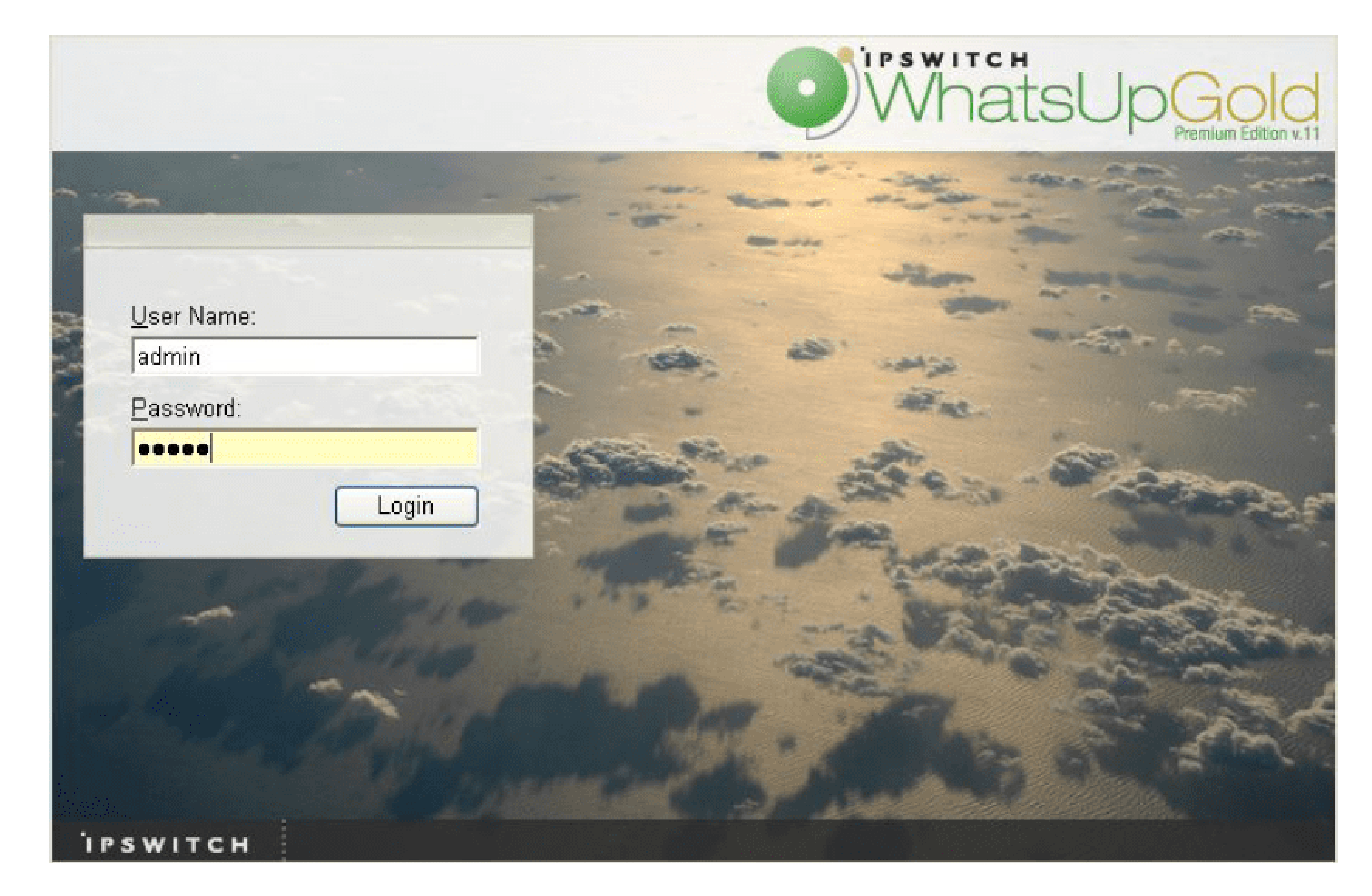
至此，经过几步简单的设置，已完成 IP 区间范围方式的设备发现操作。第 6 章中将详细介绍其他设备发现方式、设备属性配置、报警提示动作配置及报表应用等内容。

5.2.3　Web 界面模式简介

新版 WhatsUp Gold 的 Web 界面模式已经能够提供与应用程序界面一样的功能，包括配置访问凭证库、主动\被动监测库、报警与提示动作库等。除此之外，Web 模式还能根据自己的需要，配置自定义的工作界面来展示用户最感兴趣的数据，以及提供各种类型、各个层面的数据报表。

首先介绍登录 Web 界面模式。在程序安装完成后，如果未对访问 Web 模式的端口做过更改，则使用默认地址 Localhost 及默认端口 8080。直接在浏览器中输入地址 http://localhost:8080/即可访问 WhatsUp 的网页模式。或者在 WhatsUp Gold 控制台界面，通过单击查看报表按钮进入 Web 模式。打开 Web 界面后，需要输入访问的用户名和密码为 admin\admin，也可以在进入到 Web 界面后更改访问密码。Web 界面如图 5-30 所示。

登录到 Web 界面后，可看到 GO 的控制菜单，通过该菜单命令，可定位到最常用的区域，包括自定义的 Home 工作间、设备列表和报表信息。GO 菜单中，还能配置主动\被动监测库、凭证库等信息。Home 工作间如图 5-31 所示。



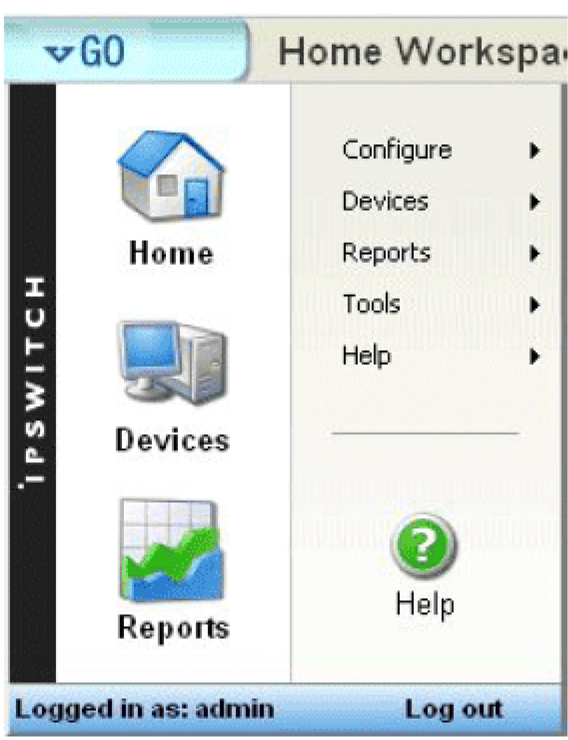


图 5-30　访问 Web 界面　　　　　　图 5-31　Home 工作间

Web 模式主界面中主要分为 3 个分页显示区域，即 Home（展示综合信息工作间）、Device（设备管理和配置界面）和 Report（报表界面），如图 5-32 所示。

图 5-32　Web 界面区域

Home Workspace：工作间区域。该界面中包含了多种统计信息和报表信息，该区域所显示的内容可根据用户的需要进行添加或布局，如图 5-33 所示。

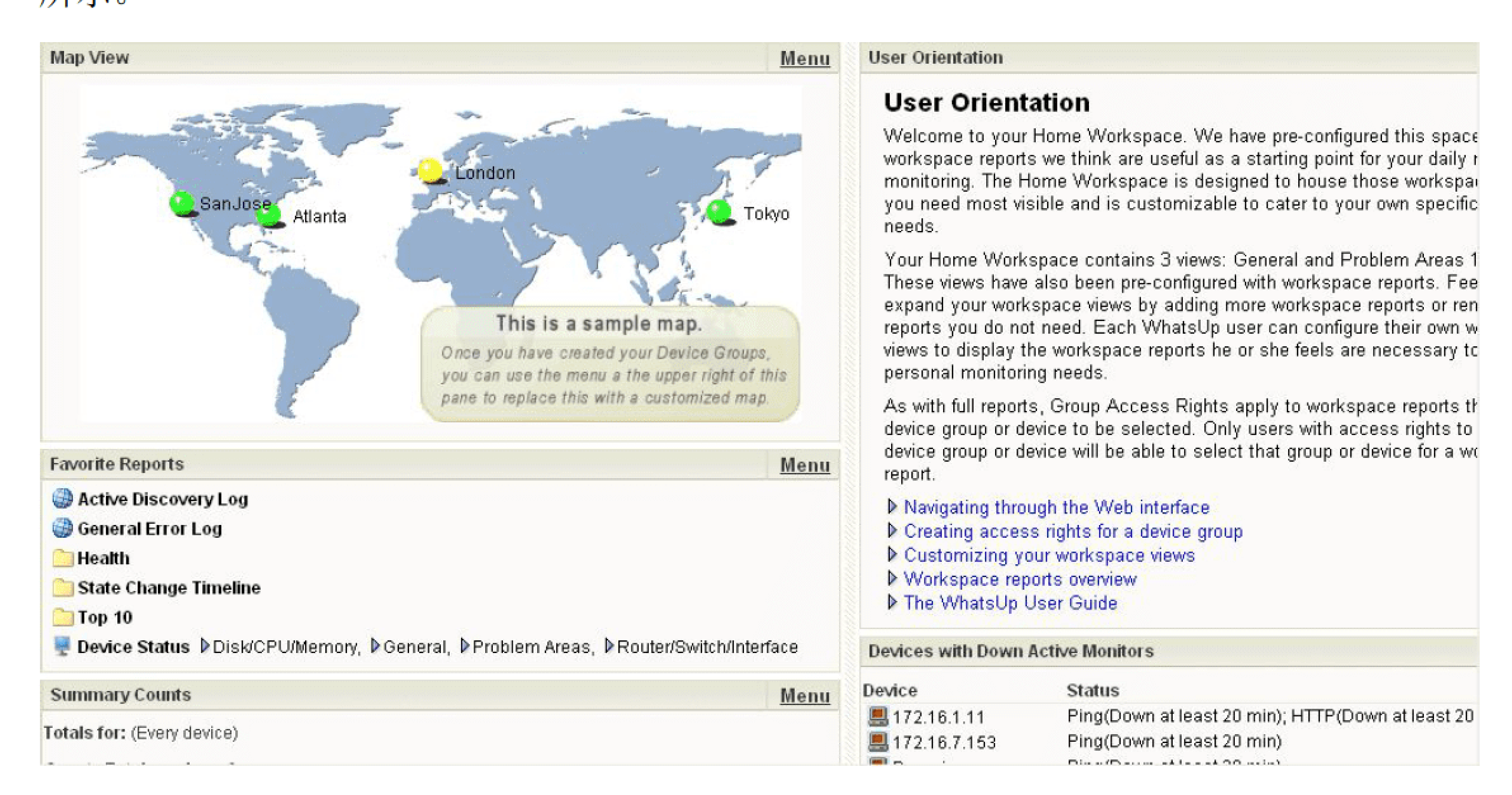


图 5-33　Web 界面模式中的 Workspace 界面

也可以在 Workspace 中自定义建立多个工作视图，并通过 Workspace View 下拉列表框选择进入各个视图界面，如图 5-34 所示。



图 5-34　切换 Workspace 视图

Device：设备列表区域。该区域中列出了所有的设备组及组中的设备。该界面提供和 WhatsUp 控制台模式中一样的功能，如图 5-35 所示。

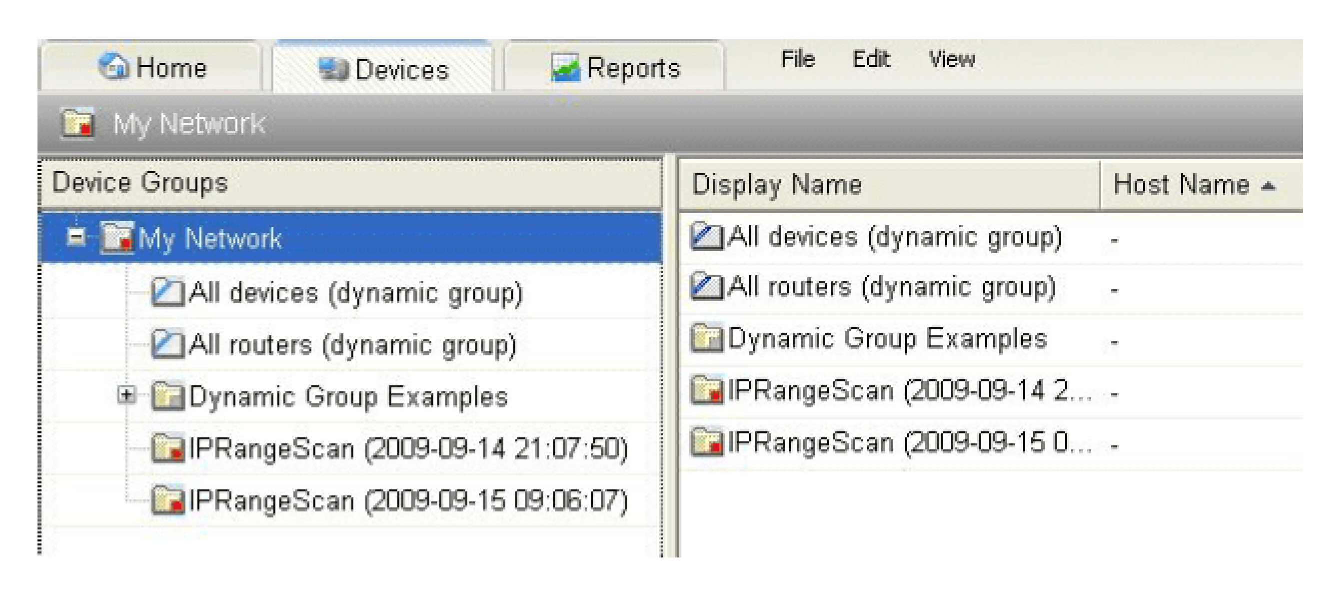


图 5-35　Web 界面中的 Device 设备界面

在设备列表界面中，可通过菜单对所选设备进行控制，包括添加设备、设备组，复制、删除设备，切换列表视图到 Map 视图等功能。也可以通过界面右上角的快捷图标进行设备和设备组的添加，如图 5-36 所示。

New Device　New Group　New Dynamic Group

图 5-36　设备界面快捷图标

Report：报表信息。该界面中，可查看各种类型、各种级别的报表信息，包括设备报表、性能报表、监测数据报表、故障信息报表等，如图 5-37 所示。

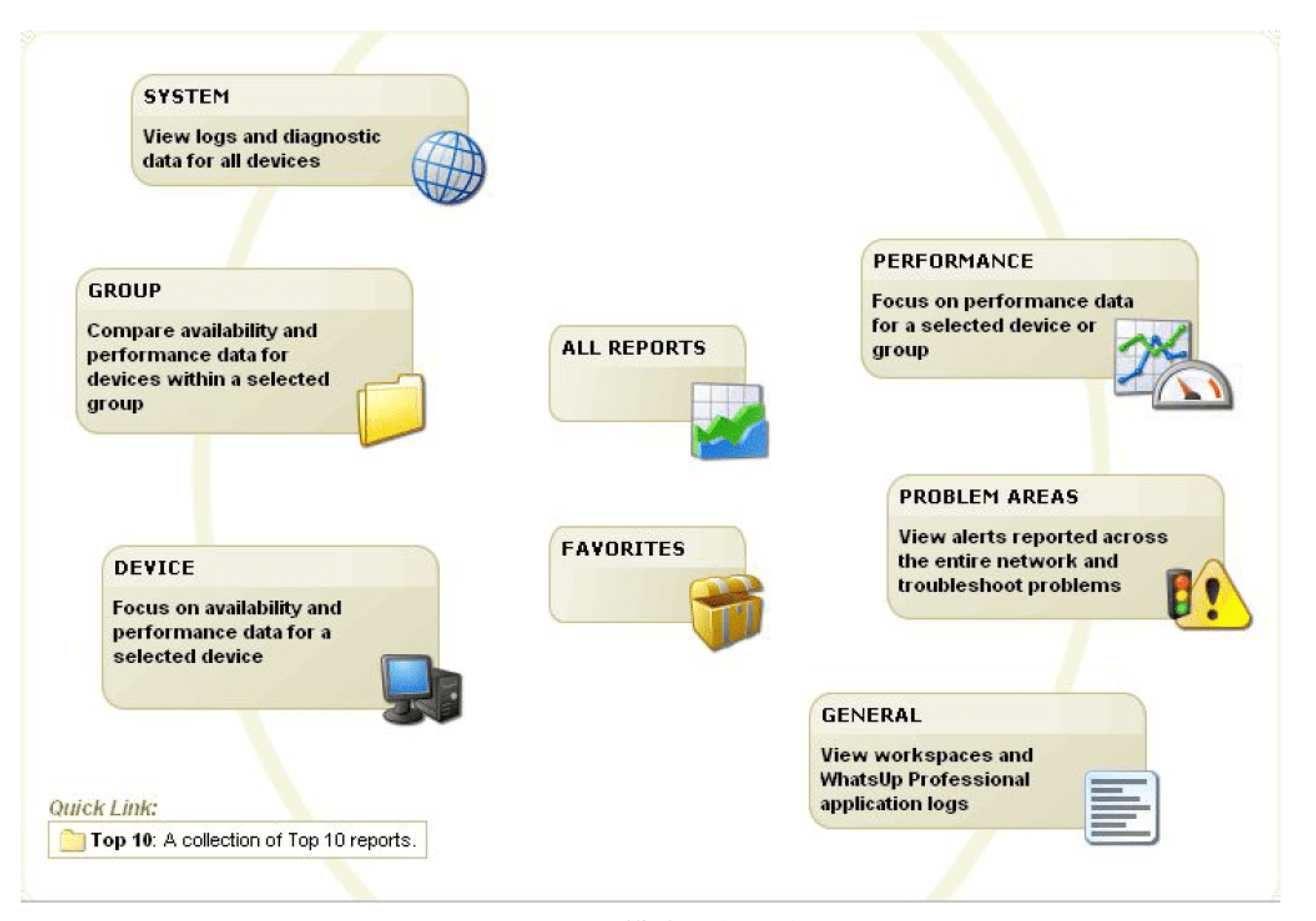


图 5-37　Web 模式下的报表界面

5.3 本章小结

本章主要介绍了 WhatsUp Gold 的安装、简单配置、快速入门和 Web 视图模式，让网络管理员对该程序的功能有初步的了解和印象，并让网管员快捷地体验该程序简单易用、结构清晰等特点。关于 WhatsUp Gold 更详细的功能、配置、应用、报表和 Web 界面使用，将在第 6、7 章中进行详细的介绍。

第 6 章 设备发现、报警设置和属性详解

本章开始详细介绍如何使用网管软件 WhastUp Gold 实现网络设备管理。首先介绍 WhatsUp Gold 的主要功能和基础配置，即查找网络设备、配置告警提示、设备属性配置等。具体内容如下：

- 扫描发现网络设备；
- 配置报警动作和报警动作组策略；
- 设备属性配置；
- 拓扑图配置；
- Web 模式应用。

6.1 扫描发现网络设备

WhatsUp Gold 支持通过多种方式查找和发现网络设备，包括使用 SNMP 智能扫描、IP 段扫描或查找同一工作组设备等方式。通过多种扫描方式的结合，能够确保发现网络中所有的设备。当查找向导发现网络设备或服务后，WhastUp Gold 会将所选监控对象存入到数据库中，并在设备列表中以虚拟设备的方式来描述网络实体。

在 WhatsUp Gold 控制台界面中，通过选择主菜单中的 File | Discover Devices 命令，打开设备发现向导，如图 6-1 所示。

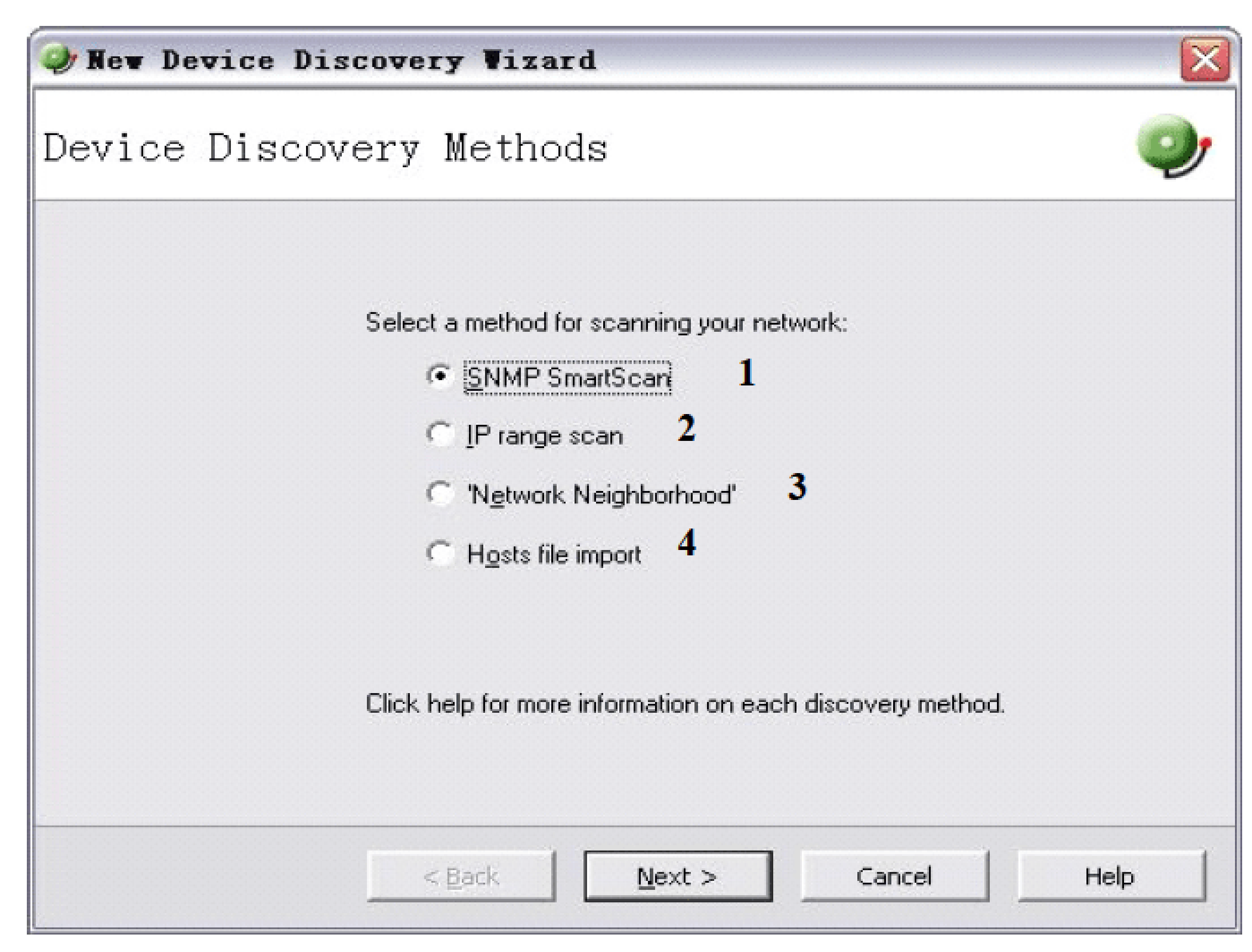


图 6-1 发现网络设备向导

WhatsUp Gold 提供了 4 种发现网络设备的扫描方式，如下：

- SNMP SmartScan：SNMP 智能扫描模式。该方式通过读取网络中的 SNMP 信息，通过开启 SNMP 服务的交换机或路由器去查找和发现网络设备。该选项为最常用的方式。
- IP Range Scan：IP 区间段扫描模式。该方式通过设置 IP 区间段的方式逐个查找设备。在 SNMP 服务不可用或 SNMP 扫描不能满足需求的时候，可使用 IP 区间段的方式。
- Network Neighborhood：查找网上邻居模式。该方式通过扫描计算机所接入的 Windows 网络查找设备，发现处于同一工作组或同一 Windows 域的其他设备。如果仅需要发现 Windows 设备，则可采用该扫描模式。
- Hosts File Import：文件导入模式。该方式通过导入一个包含主机名和 IP 地址列表的文本文件，将设备信息导入到 WhatsUp Gold 控制台和数据库中。

6.1.1 SNMP SmartScan 扫描方式

在第 1 章中已经介绍了如何在 Windows 系统、Linux 系统、及路由器和交换机上安装和开启 SNMP 服务，通过在核心交换机或路由器上的 SNMP 服务，WhatsUp Gold 可以发现网络中开启 SNMP 服务且能正常访问的设备。如果网管员只在网络分支的路由器或交换机上打开 SNMP，并通过该分支设备 SNMP 服务查找网络，那么有可能仅发现网络中一部分设备，所以推荐使用核心网络设备上的 SNMP 服务进行扫描，以保证查找到完整的设备信息。

通过 SNMP SmartScan（SNMP 智能扫描模式）方式去发现网络中的设备，需要首先知道以下知识：

- 搜索的目标网络中，提供 SNMP 服务的核心路由器或交换机 IP 地址。
- 该网络中，配置在各个网络设备上的 SNMP 社区字符串。SNMP 扫描需要提供正确的访问认证字符串，并与设备上的社区字符串相匹配，SNMP 才能够访问设备获取信息。

使用智能扫描模式添加设备的步骤如下：

（1）在扫描类型中选择 SmartScan 方式，进入凭证设置界面，如图 6-2 所示。

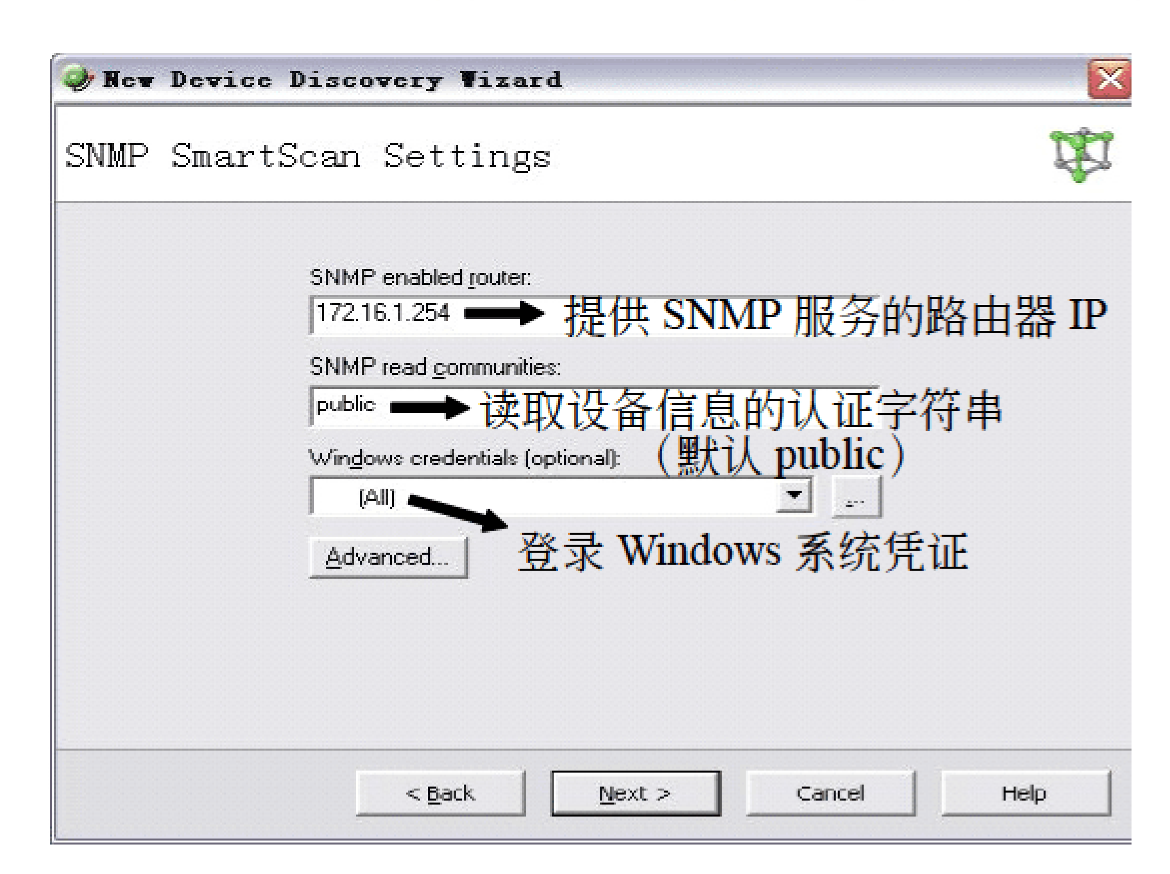


图 6-2　SNMP SmartScan 扫描方式配置

在该界面中，需要配置如下文本框内容。

SNMP enabled router：输入提供 SNMP 服务的核心路由器或交换机的 IP 地址，通过该路由器 SNMP 去搜索其他设备。

SNMP read communities：输入读取该网络设备信息的认证字符串（默认为 public），如果有多个支持 SNMP 的设备采用了不同社区字符串，那么将字符串添加到该文本框中，并以逗号分隔开。

Windows credentials（optional）：选择在查找过程中需要用到的凭证，该凭证包括 SNMP 凭证和 Windows 登录凭证。在查找设备过程中，有些 Windows 设备还需要登录认证才允许被发现或监测。Windows 设备登录认证信息（用户名和密码）可逐个添加并保存于凭证库中。此处选择 All，则在查找过程中使用库中所有的凭证；如果选择 None 选项，则在查找过程中会忽略掉那些需要登录认证的设备。

如需添加访问凭证，单击下拉框右边的【...】浏览按钮，即可打开凭证库，查看和添加凭证信息，如图 6-3 所示。

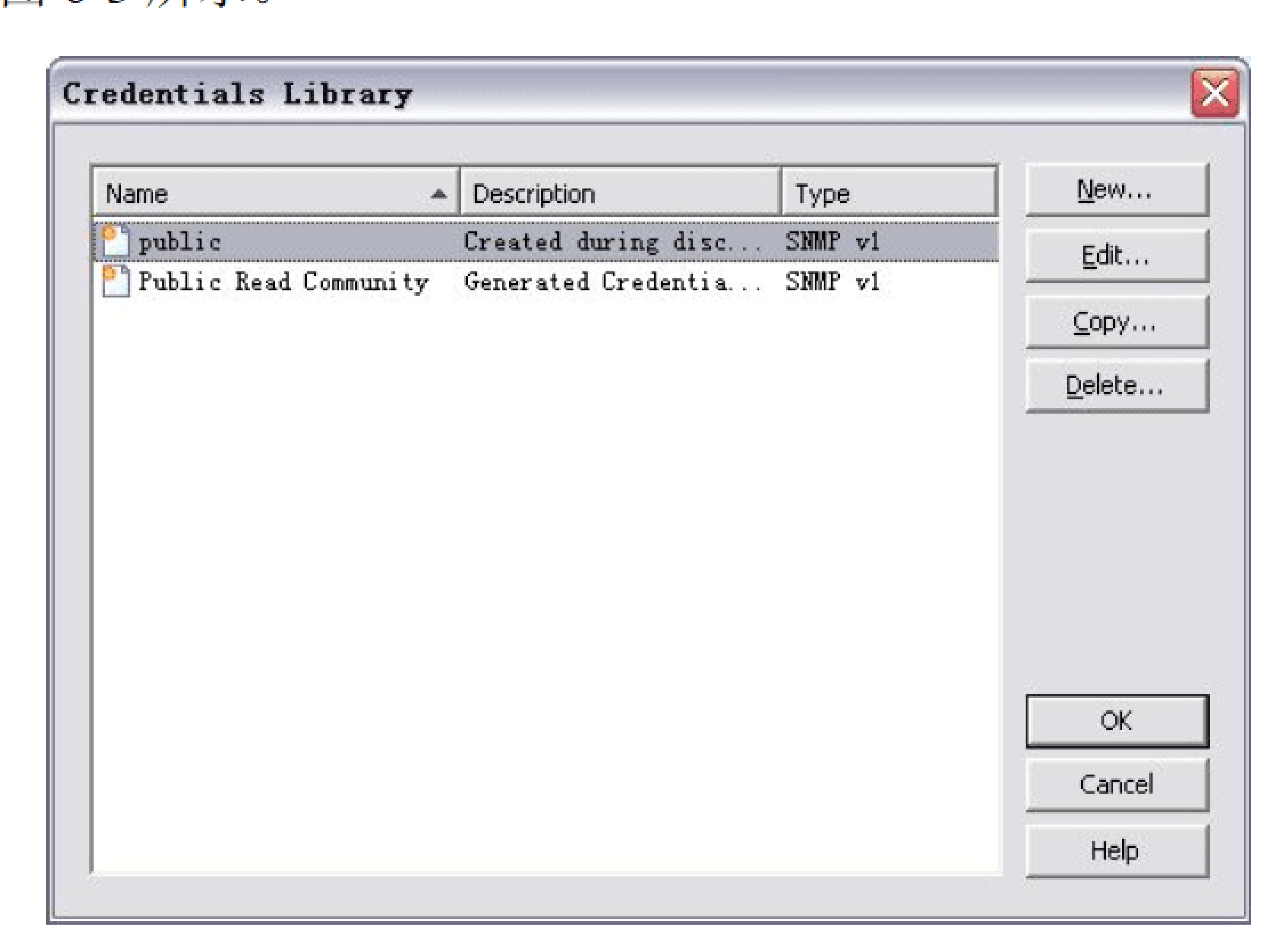


图 6-3　凭证库

在图 6-3 中，如需添加 Windows 设备访问凭证，例如为 Web 服务器添加一个登录访问凭证，可单击 New 按钮，并选择要添加的证书型为 Windows，如图 6-4 所示。

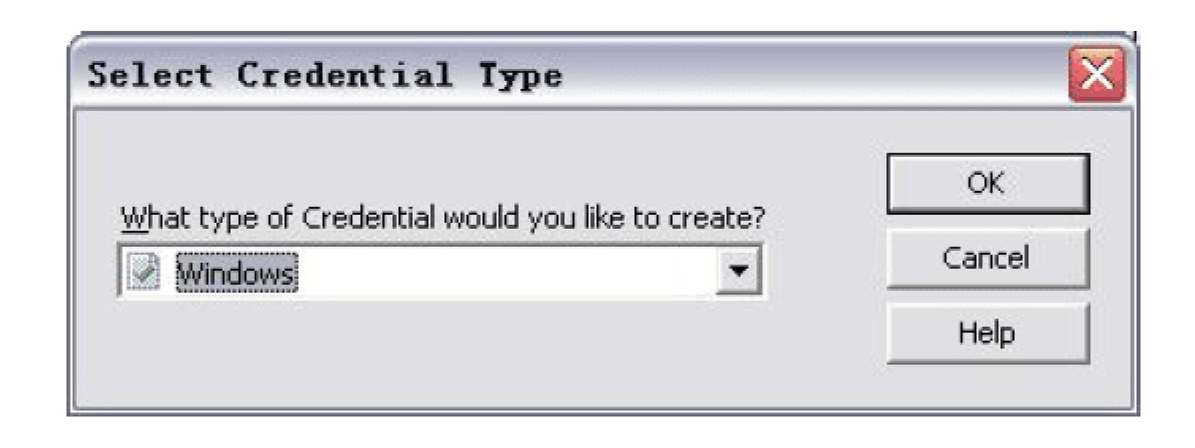


图 6-4　添加 Windows 登录凭证

确定后，进入证书设置对话框。此处输入凭证名为 Web Server，在 Domain\UserID 文本框中输入域名和 Web 服务器的域账户名，在 Password 文本框中输入登录密码，即为 Web 服务器添加了凭证。通过该凭证，SNMP 能够采集到 Web 服务器的更多信息，如图 6-5

所示。

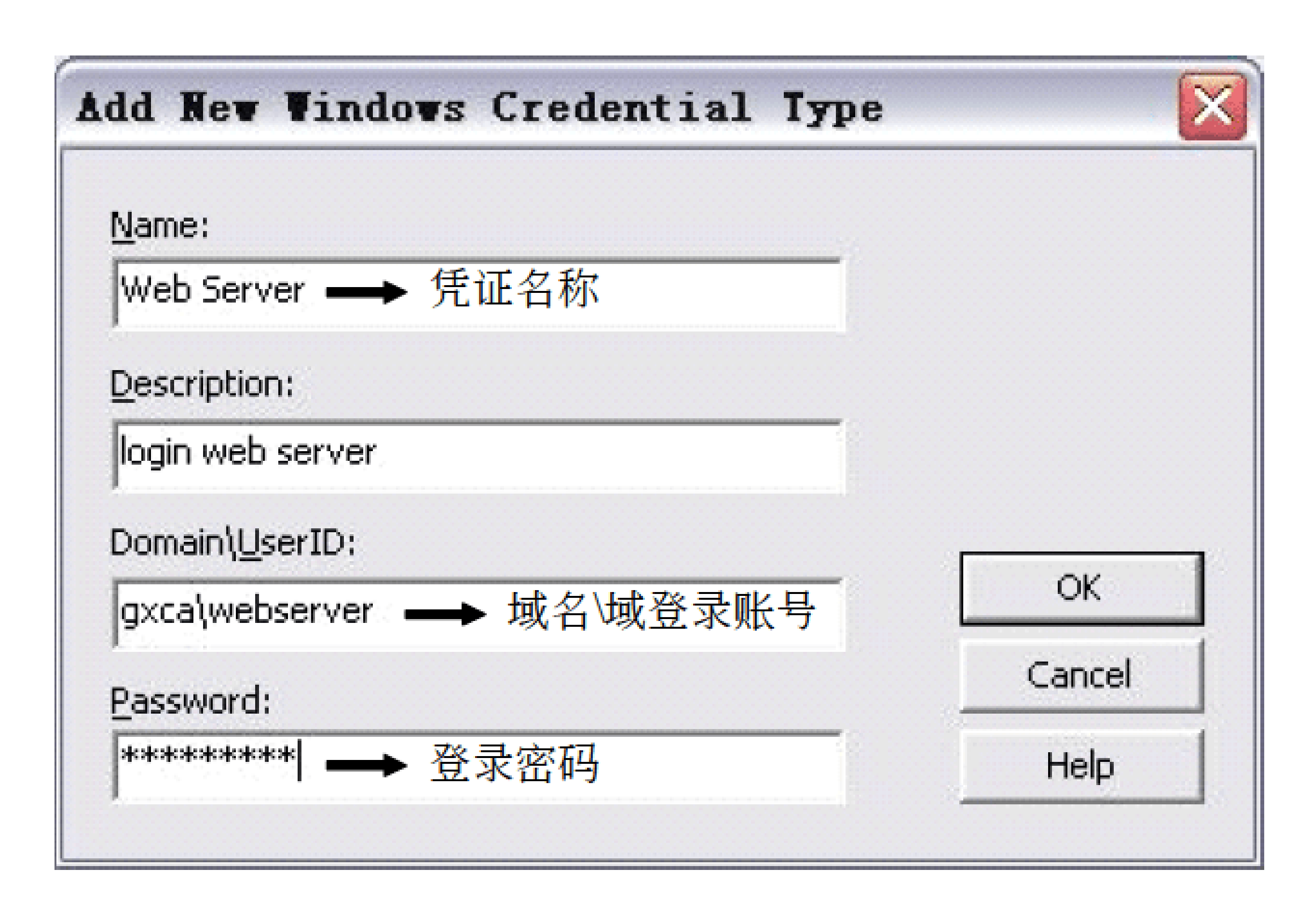


图 6-5　新建 Windows 登录凭证

（2）设置完凭证信息后进入下一步，选择在该次操作中要扫描的主动监测对象和性能监测对象，如图 6-6 所示。



图 6-6　选择要扫描的监测内容

注意：在 New Device Discovery Wizard 界面中，一定要将 Interface 选项选中。否则智能扫描结束后，在自动绘制拓扑图时，将不会生成网络设备间连线。

在如图 6-6 所示的界面中列出了要扫描的监测对象和性能对象。WhatsUp Gold 开始查找网络时，首先向 IP 地址发送一个 Ping 命令如果设备响应，则逐一扫描在 Active Monitors 和 Performance Monitors 列表框中选择的监测内容。如果设备无响应，则跳过该 IP 并执行下一个 IP 地址的查找。扫描过程结束后，某一设备响应了列表中的某几项监测内容，则

WhatsUp Gold 就为该设备增加这几项监测项目，并在轮询设备时逐一询问这几个项目的运行的状态。

注意：如果选择了 Use Comprehensive discovery 复选框，则在扫描以上监测对象时不需要提前发送 Ping 命令以确认设备是连通状态，WhatsUp Gold 将直接扫描以上服务内容，并耗费更长的时间才能完成扫描。

以下通过列表方式解释主动监测项目和性能监测项目。主动监测项目见表 6.1。

表 6.1 常用的主动监测项目及其描述

序号	类型	端口	监测对象及描述
1	DNS	53	Domain Name Service，实现对域名服务器的域名解析功能监测。如果该端口没有 DNS 服务的响应，则认为 DNS 服务停止
2	Echo	7	监测 TCP/UDP Echo 服务，该服务用于回显从该服务器端口收到的消息数据。回显服务作为网络调试和监视工具很有用。在 Windows XP\Server 2003 中需要安装组件“网络服务”|“简单 TCP/IP 服务”，才能启用 Echo 服务
3	FTP	21	监测文件传输服务 FTP
4	HTTP	80	监测 Web 服务器 HTTP 协议。该协议在当 HTTP 客户端请求建立一个到服务器指定端口（默认 80）的 TCP 连接请求时，HTTP 提供请求响应
5	HTTP Content	80	监测 Web 服务器和 Web 内容信息，包括长度、页面类型（text/html）、文件内容起始位置等
6	HTTPS	443	监测 Web 服务器。HTTPS 为加密的 HTTP 传输协议
7	IMAP4	143	监测邮件服务器。Internet 信息访问协议 IMAP4（Internet Message Access Protocol 4）为客户端提供访问远程邮件服务器上 E-mail 的服务
8	Interface	\	通过 SNMP 协议监测设备接口状态，例如接口某性能参数的常量值监测、波动率或参数值变化区间监测
9	NNTP	119	网络新闻传输协议 NNTP（Network News Transfer Protocol Overview）是使用服务器/客户机模式实现新闻的发行、查询、记录等过程的协议。运行在 Windows Server 2000/2003 系统上，Windows XP 系统不提供该服务
10	Ping	\	最简单、通用的测试命令。Ping 命令通过向目的 IP 发送一个 ICMP 请求消息，检查网络连通性和连接速度
11	POP3	110	监测邮件服务器提供的邮局协议 POP3（Post Office Protocol 3）服务是否正常。POP3 协议用于接收电子邮件
12	Radius	1465	监测 Radius 服务器。远程用户拨号认证系统 Radius（Remote Authentication Dial In User Service）服务安装在 Windows Server 2003 系统上，并要求安装 Internet 验证服务网络组件和证书服务，采用 C/S 架构。它应用于包括 ADSL 上网、小区宽带上网、IP 电话、VPN 连接认证方面
13	SMTP	25	监测邮件服务器提供的简单邮件传输协议 SMTP（Simple Mail Transfer Protocol）服务是否正常。SMTP 协议用于发送电子邮件
14	SNMP	\	监测 SNMP 服务是否正常运行。该监测询问 SNMP 服务器，并分析返回值
15	Telnet	\	监测远程服务器上 Telnet 服务是否正常或是否允许
16	Time	37	监测时间服务器。RFC868 时间协议（Time Protocol）规范了一个时间服务标准， 时间服务器在端口 37 上监听连接，当客户端连接建立后，服务器返回一个 32 位的时间值，然后关闭连接

性能监测项目内容及其描述见表 6.2。

表 6.2　常用的性能监测项目及其描述

序号	性能监测对象	描　　述
1	CPU Utilization	CPU 利用率
2	Disk Utilization	磁盘利用率
3	Interface Utilization	接口带宽利用率
4	Memory Utilization	内存利用率
5	Ping Latency and Availability1	Ping 操作的响应时间和可用性

注意：如果要主动监测 Echo 服务，首先要在客户端启用该服务。在 Windows 系统中安装组件【网络服务】|【简单 TCP/IP 服务】后，即可启用 Echo 服务，如图 6-7 所示。



图 6-7　安装 Echo 服务

实例：在监测内容选择中，选择了 POP3 和 SMTP 两项主动监测，并扫描到 Exchange 服务器提供 POP3 服务和 SMTP 服务（对 POP3/SMTP 扫描做出响应），那么扫描结束后程序自动为 Exchange 服务器添加了这两项监控内容，并通过轮询的方式对该两项服务进行定时询问。

查看邮件服务器的主动监测项目列表，可看到包含了这两项监测内容，如图 6-8 所示。

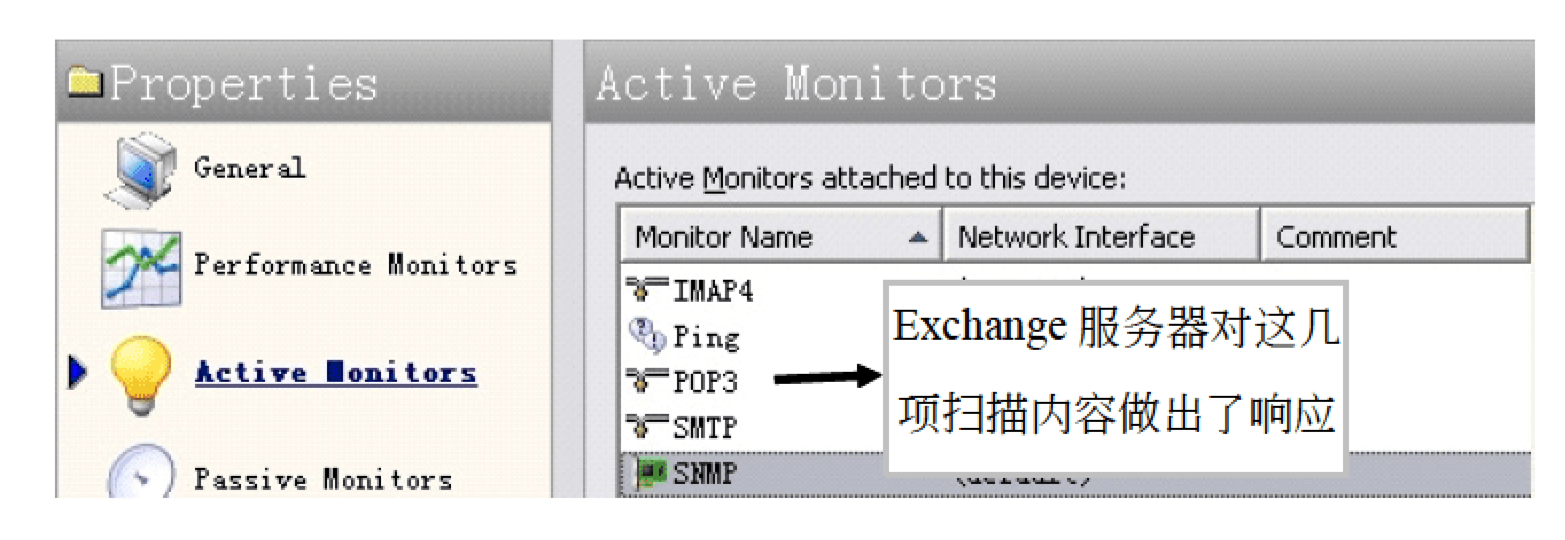


图 6-8　扫描结束后，查看设备属性中的主动监测内容

（3）选择监测内容后进入下一步，即可开始执行网络设备扫描。扫描结束后将在

Devices to Monitor 对话框中显示此次扫描发现的设备（如图 6-9 所示）。如果某些设备曾经被 WhatsUp 发现过并存入到数据库中，那么在列表中建立的是该设备的快捷方式。选择需要监测的网络设备后选择下一步，这些设备信息将被存储到数据库中。

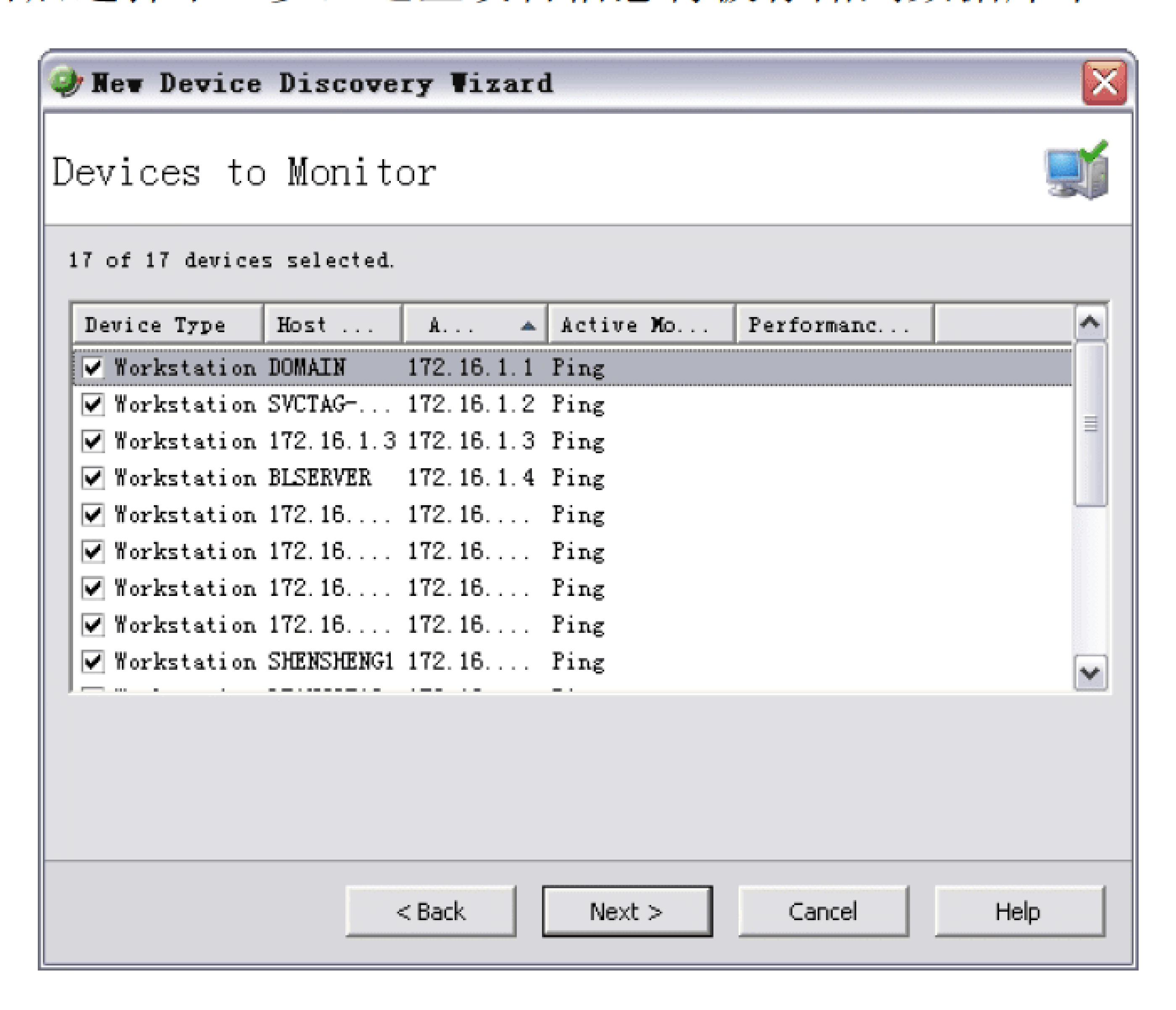


图 6-9　扫描网络发现的设备列表

注意：*每次执行扫描方式都会形成一个扫描记录，并生成一个设备组。再次扫描过程中如果发现了重复的设备，那么该次扫描将会添加已存在设备中的快捷方式作为本组设备成员。*

需要注意的是，当设备被发现后，WhatsUp Gold 通过询问设备的对象标识 OID（如 1.3.6.1.2.1.1.2）。该对象标识是网络设备供应商的身份标识。如果设备响应了询问，则表示该设备 SNMP 服务可用；如果设备对于 OID 的询问未做出响应，那么 WhatsUp 将逐一扫描之前选择的主动监测和性能监测项目。

同时，在所有类型的 Windows 凭证列表中，只要某一个 Windows 登录凭证能够访问到任何一台设备，或者设备响应了任何一个基于 SNMP 凭证的主动监测项目或性能监测项目，则凭证为正确合法。WhatsUp Gold 将获取并记录设备的 OID 值或监测项目 OID 值，该凭证会被加入到凭证库中，设备则被添加到设备列表中。

（4）选择要监测的设备后进入报警提示配置对话框。通过配置提示，当设备状态发生变化时（如停止运行、网络中断、服务停止、服务启动），WhatsUp Gold 会发出报警提示信息（如声音告警、邮件提示、弹出提示框等）或者提示动作的组合（如同时执行多项报警动作）。组合的报警提示动作被称为动作策略。

在首次使用 WhatsUp Gold 时，报警动作配置界面未包含任何动作策略，需要自行建立报警提示动作或动作策略。此处选择从系统默认包含的报警动作中建立一个新的动作策略，如图 6-10 所示。关于动作策略的详细配置将在本章“6.3 节报警动作及策略配置”部分详细介绍。



图 6-10　为查找到的设备增加报警动作策略

（5）单击 Next 按钮，进入下一步，选择在设备 5 分钟无响应和重新响应时，执行声音报警提示，如图 6-11 所示。

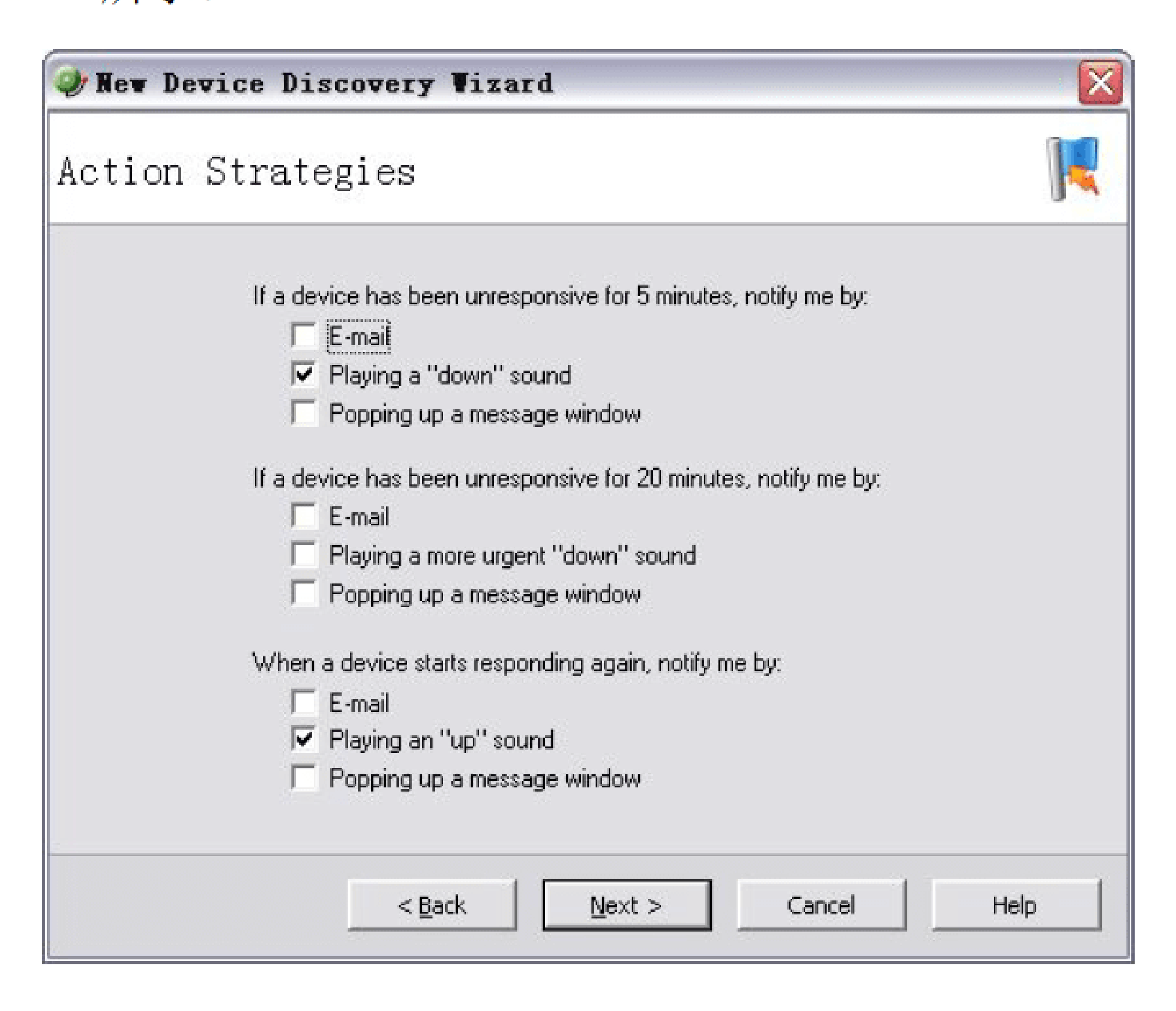
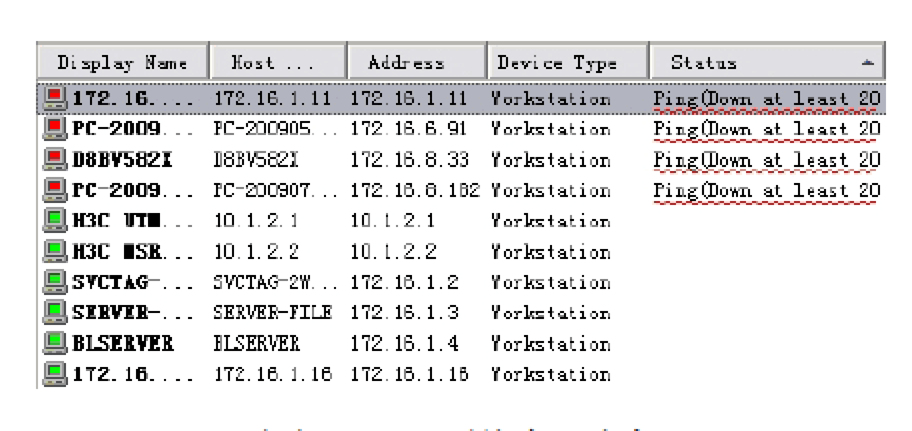


图 6-11　选择执行声音报警提示动作

选择这两项报警动作后，即为该设备添加了一个报警动作策略。选择下一步可为该策略命名。该策略建立后，将被保存于动作库中供再次调用。策略建立完成后，则完成了 SNMP SmartScan 方式的扫描操作，WhatsUp Gold 会将选择的设备对象添加到数据库中，并在程序主界面中生成设备列表，如图 6-12 所示。



Display Name	Host ...	Address	Device Type	Status
172.16....	172.16.1.11	172.16.1.11	Workstation	Ping(Down at least 20
PC-2009...	PC-200905...	172.16.6.91	Workstation	Ping(Down at least 20
D8BV582I	D8BV582I	172.16.8.33	Workstation	Ping(Down at least 20
PC-2009...	PC-200907...	172.16.8.182	Workstation	Ping(Down at least 20
H3C UTM...	10.1.2.1	10.1.2.1	Workstation	
H3C MSR...	10.1.2.2	10.1.2.2	Workstation	
SVCTAG-...	SVCTAG-2W...	172.16.1.2	Workstation	
SERVER-...	SERVER-FILE	172.16.1.3	Workstation	
BLSERVER	BLSERVER	172.16.1.4	Workstation	
172.16....	172.16.1.16	172.16.1.16	Workstation	

图 6-12　设备列表

6.1.2 IP Range Scan 扫描方式

当网络设备 SNMP 服务不可用或者 SNMP 扫描方式无法满足需要时，可采用 IP 地址段扫描方式。该方式中，WhatsUp Gold 将逐一询问地址区段内的每一个 IP 地址，查找将耗费更多时间。选择 IP Range Scan 方式后，进入 IP 地址段配置界面，需要输入起始 IP 地址和结束 IP 地址，如图 6-13 所示。

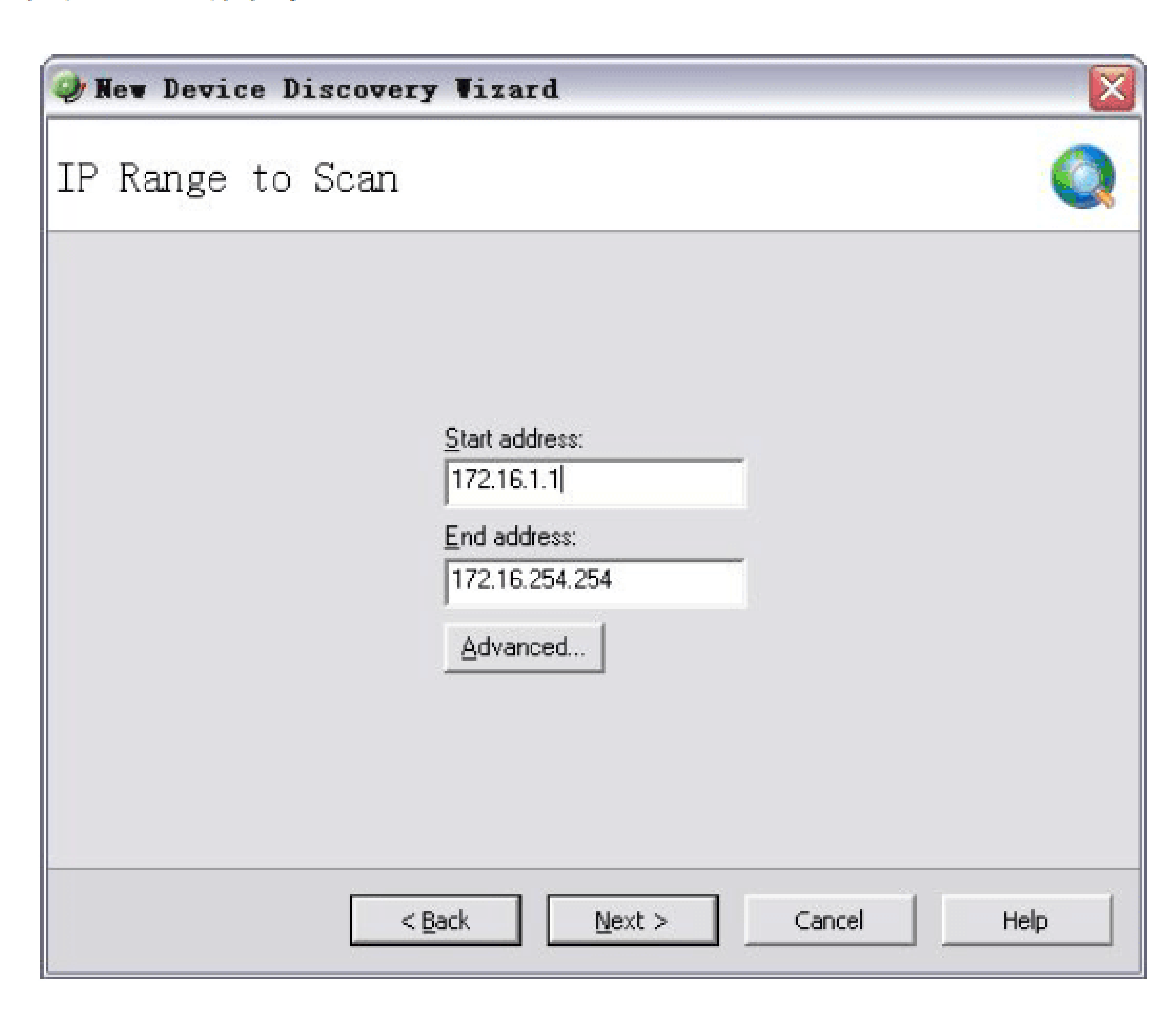


图 6-13　IP 地址段扫描查找方式

输入 IP 地址段后，单击 Next 按钮进入下一步 IP 区间扫描方式。该方式同样需要输入访问网络设备的社区字符串，以及选择 Windows 登录凭证为 All 选项，如图 6-14 所示。同样，在主动监测项目和性能监测项目选择界面，需要根据网络中可能存在的服务进行选择。

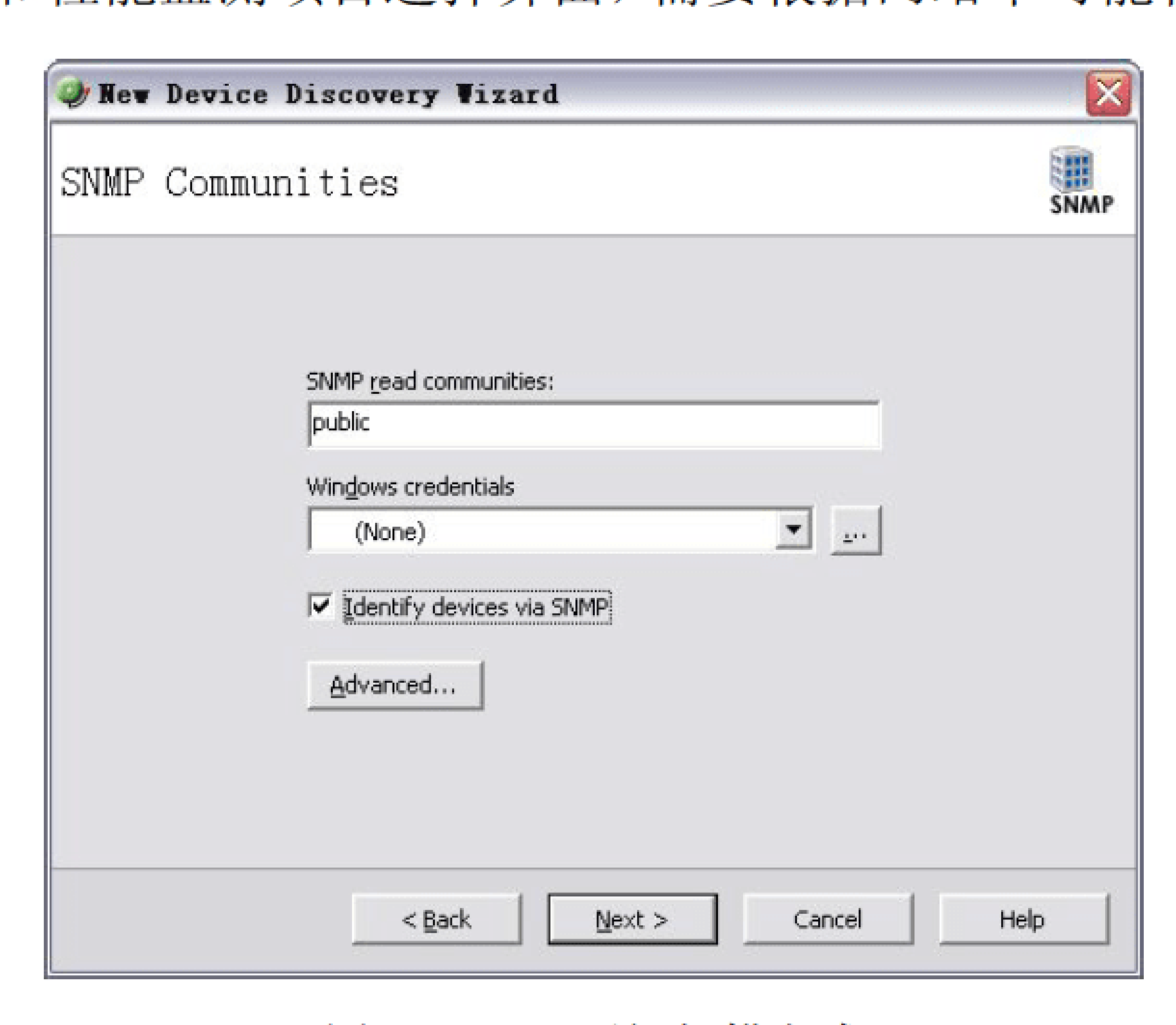


图 6-14　IP 区间扫描方式

选择要扫描的监测对象后即开始扫描查找网络设备。后续的报警动作设置方式与 SNMP 智能扫描方式一致。

6.1.3 Network Neighborhood 查找网上邻居方式

可以通过扫描网管计算机所接入的 Windows 域或工作组来查找设备。使用该方式仅能发现 Windows 系统设备。如果安装 WhatsUp Gold 的网管计算机接入到的是 Windows 域环境中，那么 WhatsUp Gold 会自动搜索到域名。如果接入的是工作组中，则 WhatsUp Gold 自动搜索到工作组名，如图 6-15 所示。

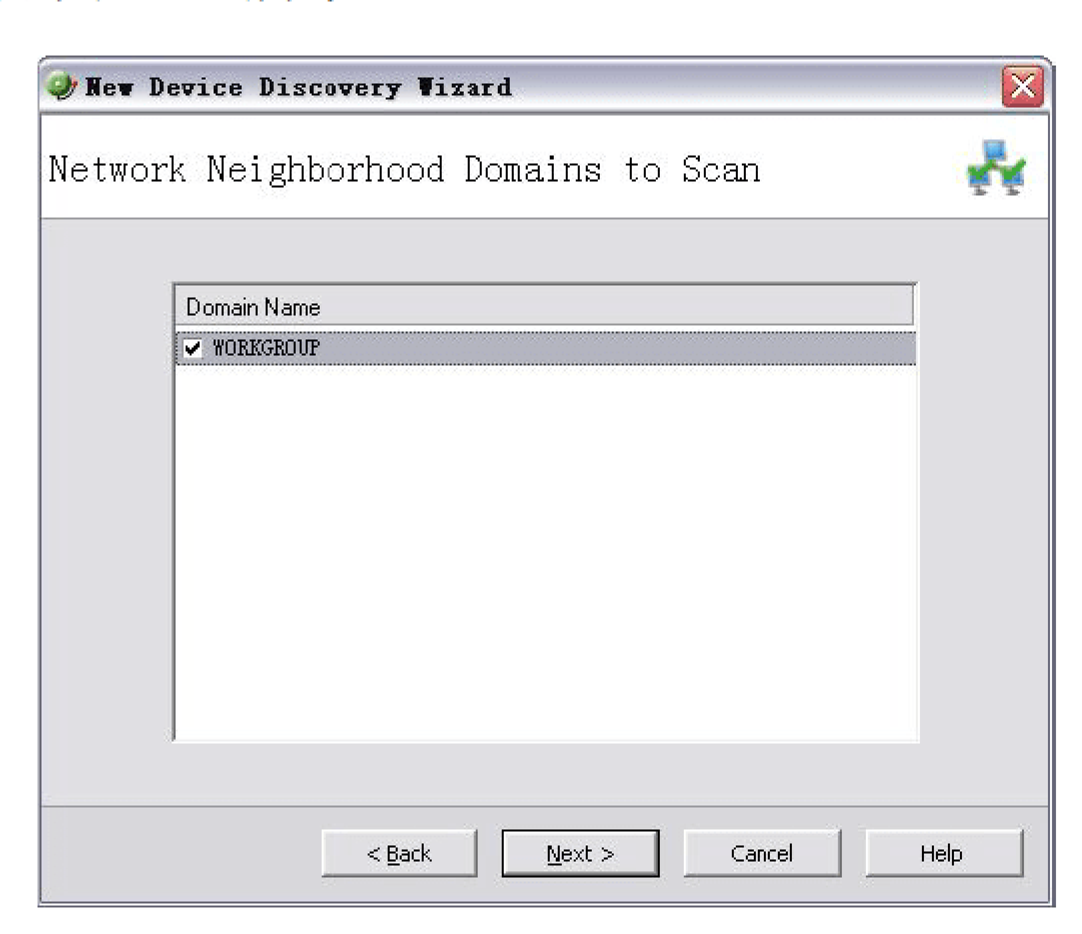


图 6-15 查找邻近节点方式

单击 Next 按钮，WhatsUp Gold 即开始扫描 Windows 域或工作组内的网络设备。

6.1.4 Hosts File Import 文件导入方式

该方式通过导入 Windows hosts 文件的方式进行设备添加。Hosts 文件中包含了网络设备的 IP 地址和 Host name（主机名）信息，以及 IP 地址与主机名的映射关系。该方式能够将列表中的设备信息直接导入到 WhatsUp Gold 程序中，如图 6-16 所示。

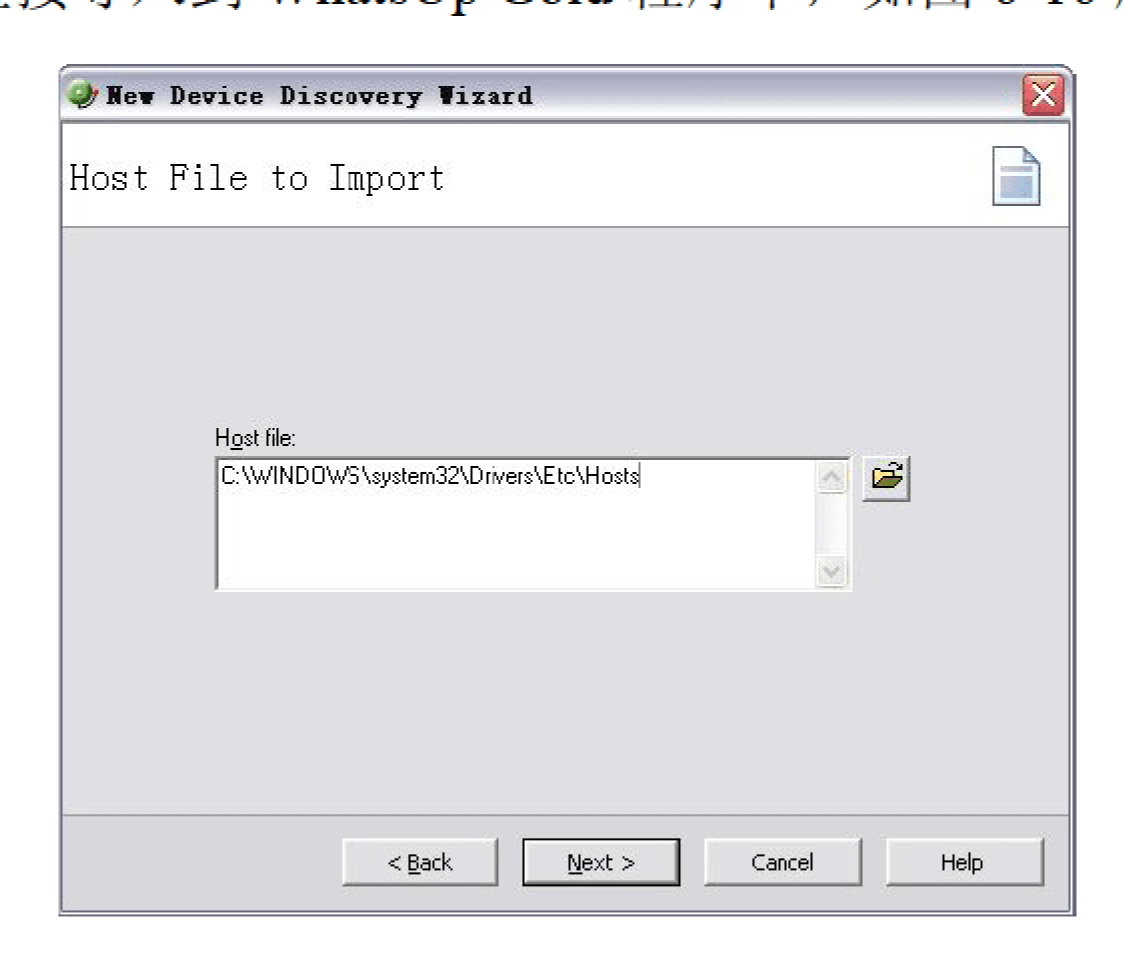


图 6-16 Hosts File 文件导入

6.1.5 手动添加设备到设备组中

除了以上 4 种方式可以添加网络设备外，WhatsUp 还提供了另外两种添加单独设备的方式。

第 1 种方式：在控制台的 Device View 或 Map View 界面中，右击打开快捷菜单，选择 New Device 命令添加单独的网络设备（或在程序界面上选择主菜单 File | New Device 命令添加设备），如图 6-17 所示。

第 2 种方式：在展开控制台左边 Device Types（Basic）的面板中（如图 6-17 所示）列出了常见的网络设备标图。将需要添加的设备图标拖至 Device View 或 Map View 窗口中，即能弹出添加设备对话框，如图 6-18 所示。



图 6-17 手动添加设备

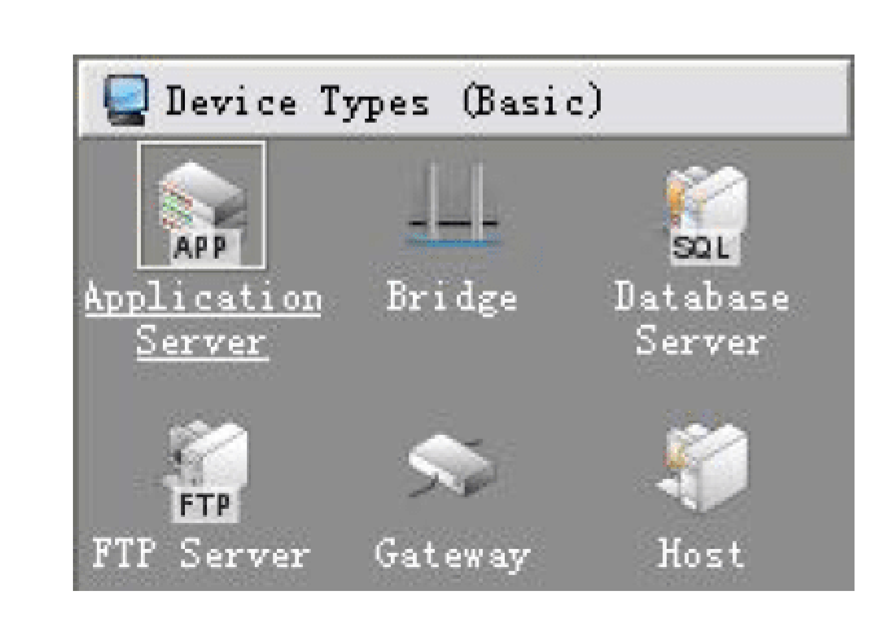


图 6-18 设备类型图标

如果需要配置设备类型图标，则选择主菜单中的 Configure | Device Type 命令，在弹出的窗口中列出了所有 WhatsUp Gold 提供的设备类型列表。可根据需要对其进行修改或者增加自定义的设备类型和图标，如图 6-19 所示。

手动添加单独设备时，只需要在弹出的对话框中输入设备的 IP 地址或主机名，WhatsUp Gold 便会扫描和分析该 IP 和 Host Name。如果该扫描操作并没有发现指定设备，程序会询问是否仍要添加该设备。选择是后，仍可以将该未知的设备加入到设备列表中，但其状态显示为无法连接。

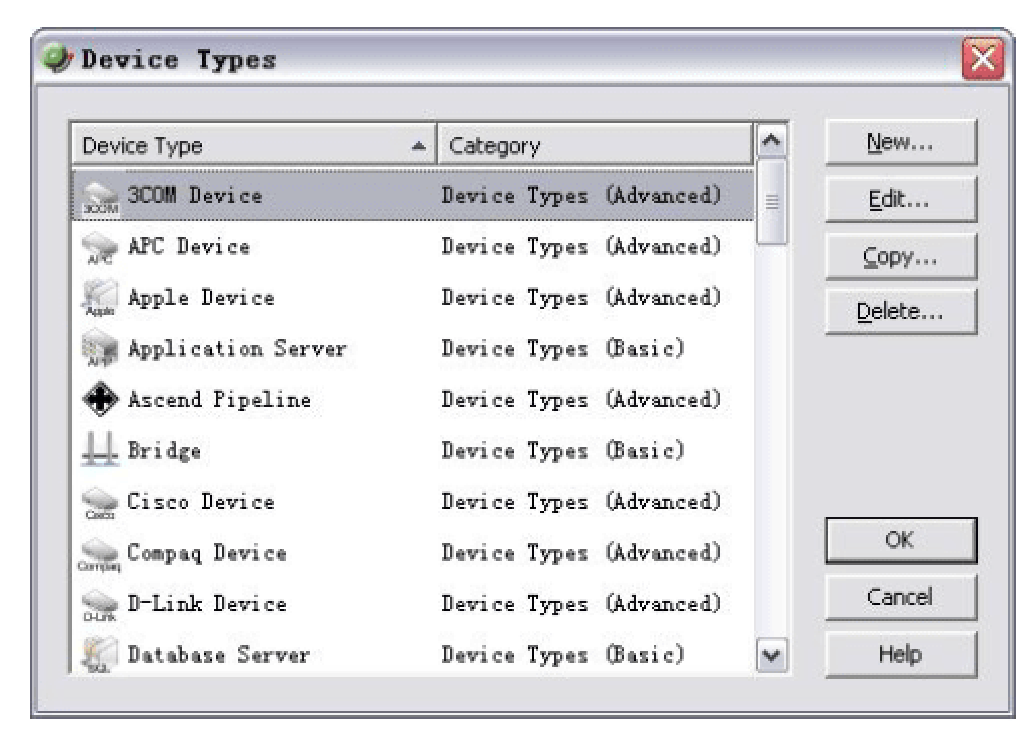


图 6-19 设备类型管理

6.1.6 制定自动查找设备任务

如果管理的网络中不断有设备接入，或者网管员希望随时掌握网络设备的接入情况，则可以制定一个自动查找设备的任务，指定该任务在每周的某一时刻执行查找任务。设置步骤如下：

（1）选择主界面中的 Configure | Active Discovery 命令，在弹出的界面中添加自动查找设备的任务，如图 6-20 所示。

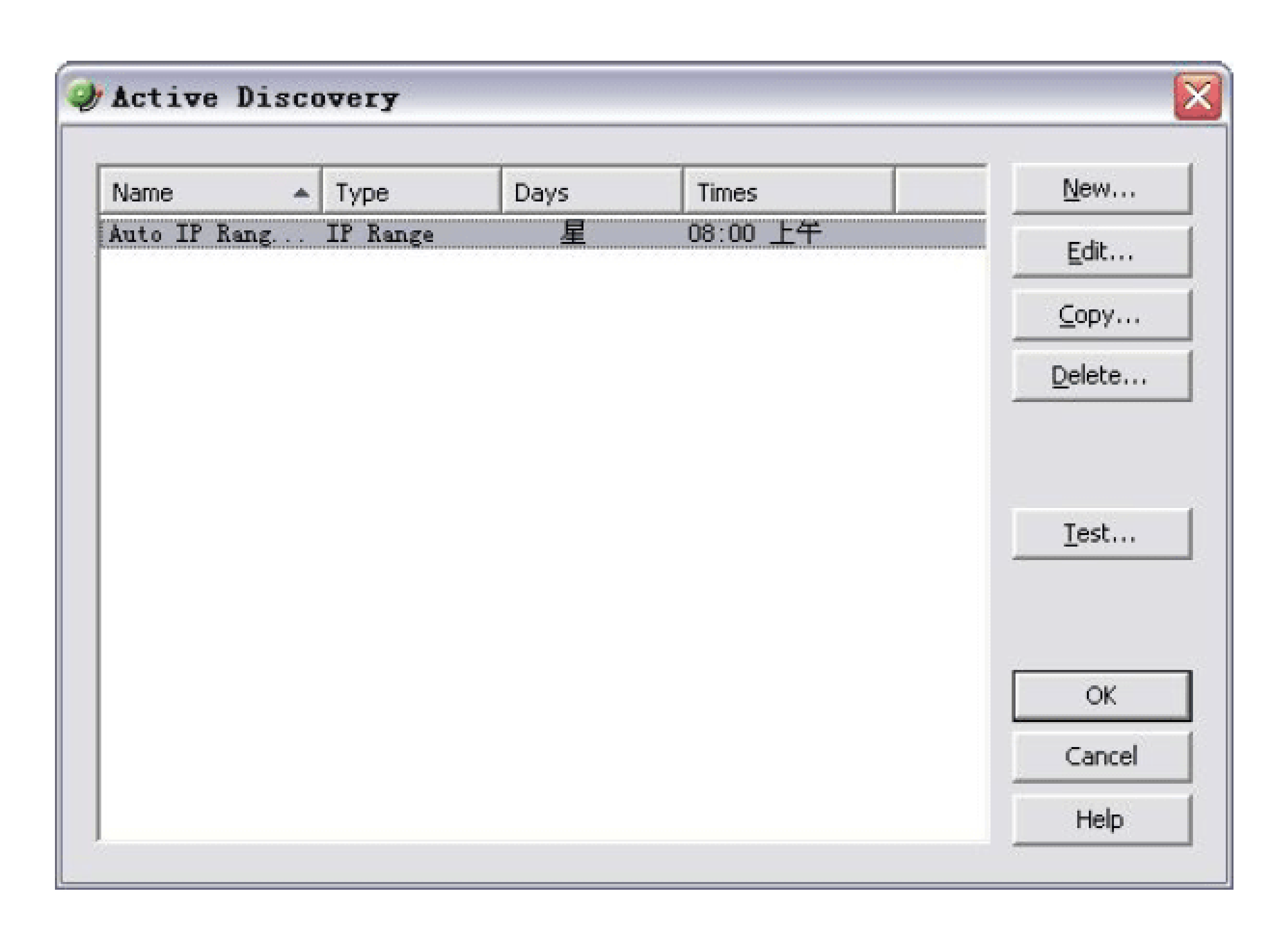


图 6-20　自动查找任务界面

（2）单击 New 按钮，并在弹出的界面中输入新建的任务名称。单击 OK 按钮进入下一步，设置执行扫描任务的时间。此处设置为每周日的早 8:00 执行一次扫描任务，如图 6-21 所示。

（3）选择任务执行时间后，WhatsUp Gold 会将查找结果通过 E-mail 方式发送至网管员的邮箱，所以需要设置接收邮件的地址及查找方式的选择（包括 SNMP 扫描和 IP 段扫描两种选项）。后续设置与前面查找添加设备的设置一样，此处不再详细介绍了。

如果需要编辑该自动查找任务，在 Active Discovery 任务列表中选择该任务弹出配置界面（如图 6-22 所示），可对任务的执行计划时间、扫描方式、扫描对象等配置做更改。

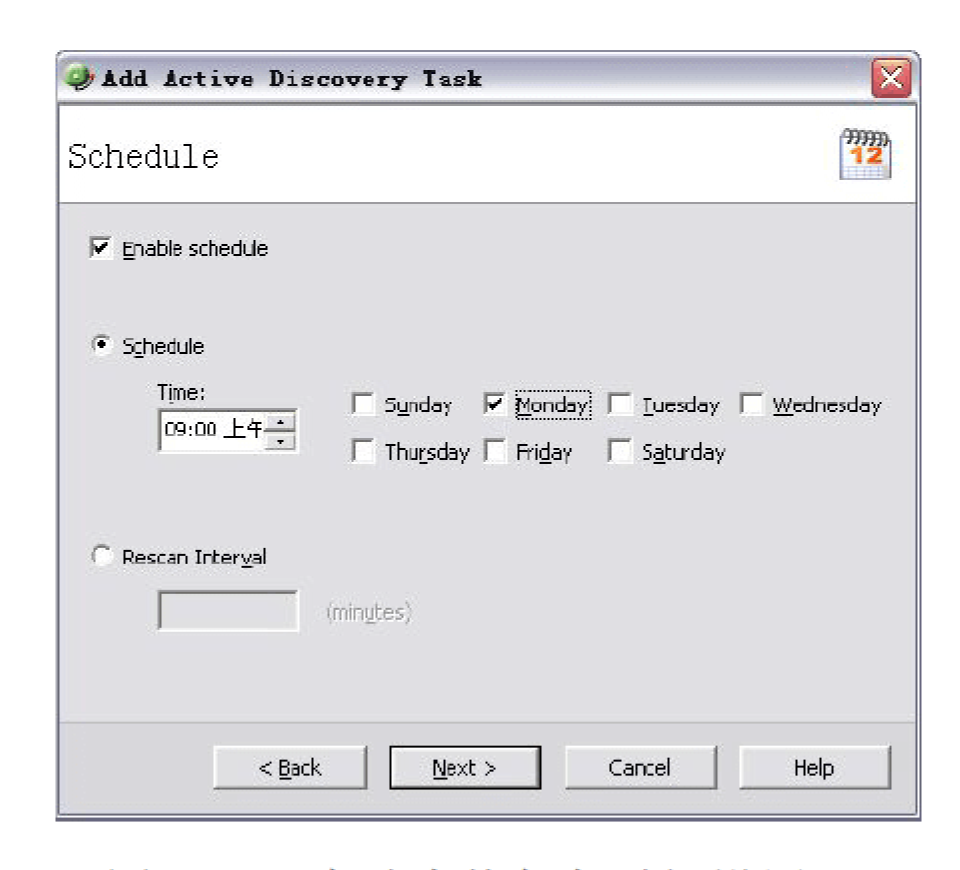


图 6-21　自动查找任务时间设置

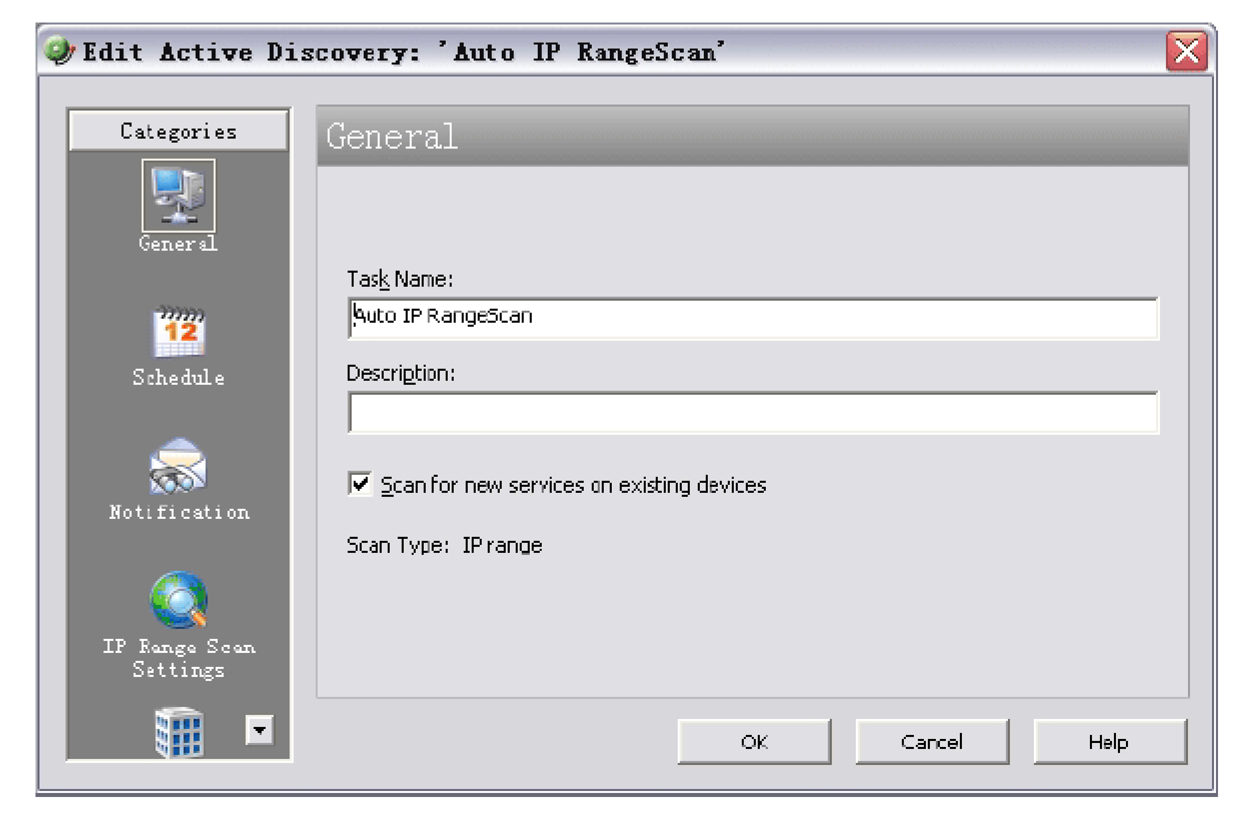


图 6-22　编辑自动任务

6.2 设备属性详解

6.2.1 设备状态图标简介

在主界面中的设备列表中会出现如下代表设备不同状态的图标，如表 6.3 所示。

表 6.3　设备图标类型列表

图标	显 示 颜 色	状 态 说 明
	绿色	该设备的所有监测对象被认为都是正常状态
	绿色	快捷方式，该设备同时存在于另一个设备组中
	红色带绿色图标	设备被认为是停止运行状态的。因为其中一个或几个重要监控对象无响应，绿色小图标表示至少有一个监控是有响应的
	绿色带红色图标	设备存在于另一个组中，该设备中至少有一项监测对象是无响应，同时至少有一个监控项目是启动活动状态的
	橘红色	设备处于日常维修模式
	带红色图标文件夹	该设备组中包含至少有一个设备处于停止运行状态
	灰色图标文件夹	该设备组无设备
	绿色粗体名称	在图标中显示粗体的设备名字，表示设备状态有改变，同时该状态的变更是未经过认可的

6.2.2　设备属性概要

在 WhatsUp Gold 程序中，设备列表通过虚拟的方式来描述实体设备，包括计算机或工作站、服务器、路由器、交换机等。在设备列表中，可以通过配置设备属性来更改单个设备描述、配置告警方式、添加监测行为等。以下将详细介绍设备的各项属性配置。

首先介绍设备常规属性。在设备列表中双击某设备，或者在设备上右击选择 Properties 菜单命令，打开设备属性配置窗口，在左边目录中列出了该设备所有可配置的属性，选择 General 选项，将显示常规选项属性，如图 6-23 所示。

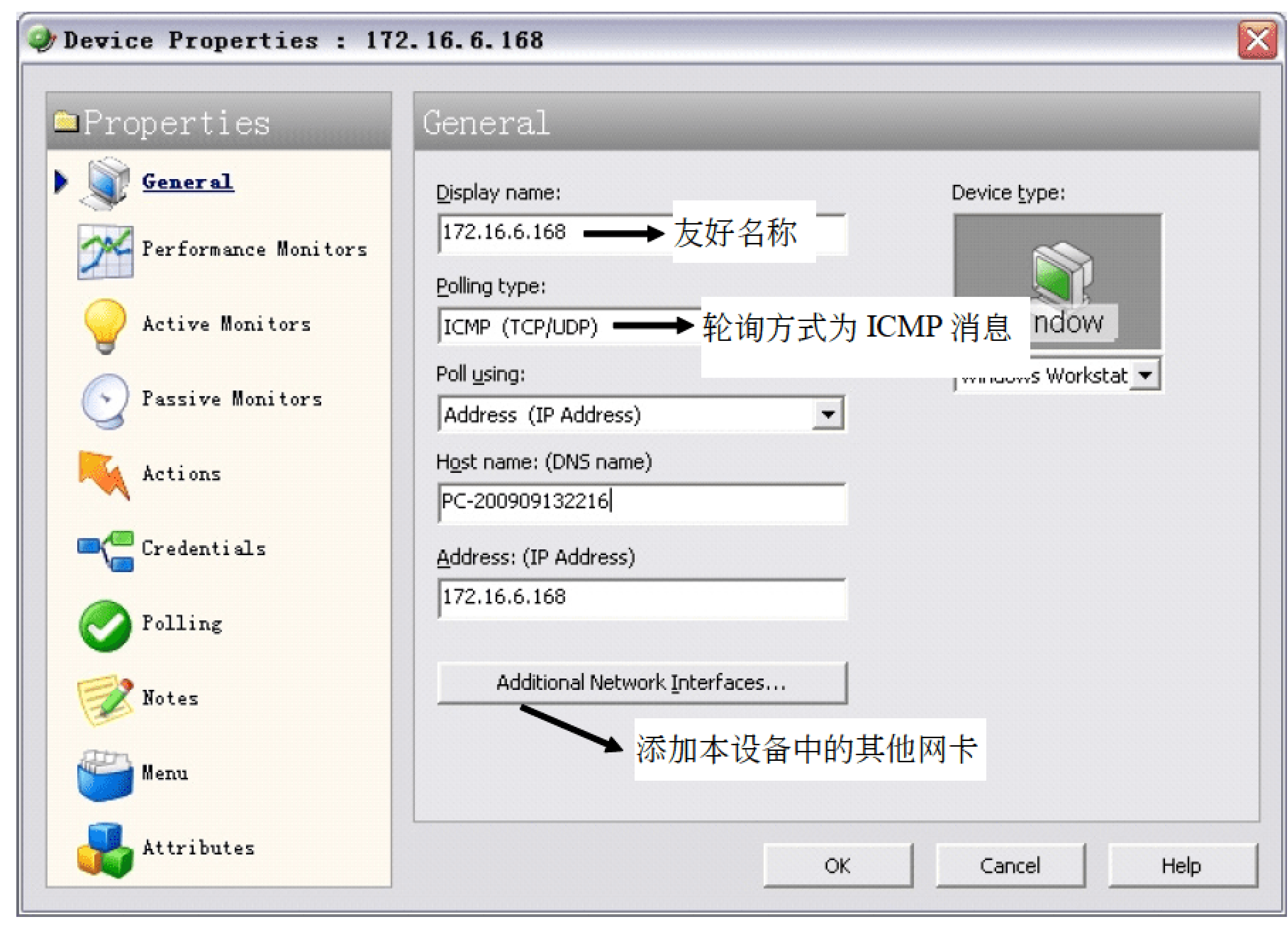


图 6-23　设备基本属性

常规设置界面包含了设备的基本属性，可自定义设备友好名称。在轮询机制中。可选择轮询设备采用的访问协议。常用的是ICMP 协议，即通过向设备的 IP 地址发送 Ping 数据包询问设备是否响应。如果设备响应了询问，则该设备状态为 Up，否则为 Down。

在图 6-23 的右上角，可根据设备的实际情况，为其选择设备类型图标。选择图标下拉列表，即可进行图标选择，如图 6-24 所示。

如果该设备包含多个网卡，可通过下方的 Additional Network Interface 按钮添加其他网卡接口地址，将接口信息添加到监测中。

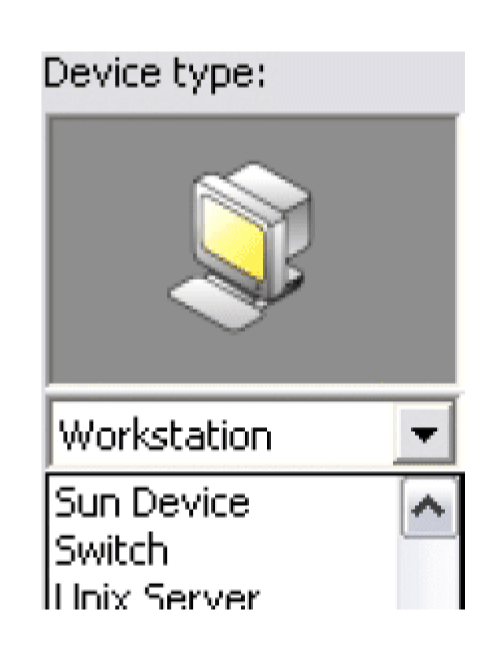


图 6-24　设备图标列表

6.2.3　Performance Monitors 性能监测

WhatsUp Gold 应用 SNMP 进行网络和设备监测，具体包括性能监测、主动监测和被动监测 3 类方式。首先介绍性能监测方式。SNMP 通过设备上运行 SNMP Agent 代理获取设备性能信息。例如，访问 SNMP Agent 可获取服务器硬件资源利用率、端口信息、路由表和网络设备流量等信息，这些信息就是 SNMP Objects 对象的信息，以标准格式存储于 MIB 中，WhatsUp Gold 按照轮询的时间间隔去访问 Agent，获取这些对象的性能参数。

（1）在设备属性界面，选择 Performance Monitor 选项，在 Enable global performance monitors 列表中列出了常用的性能监测内容，包括 CPU、磁盘、接口、内存利用率和 Ping 操作，如图 6-25 所示。

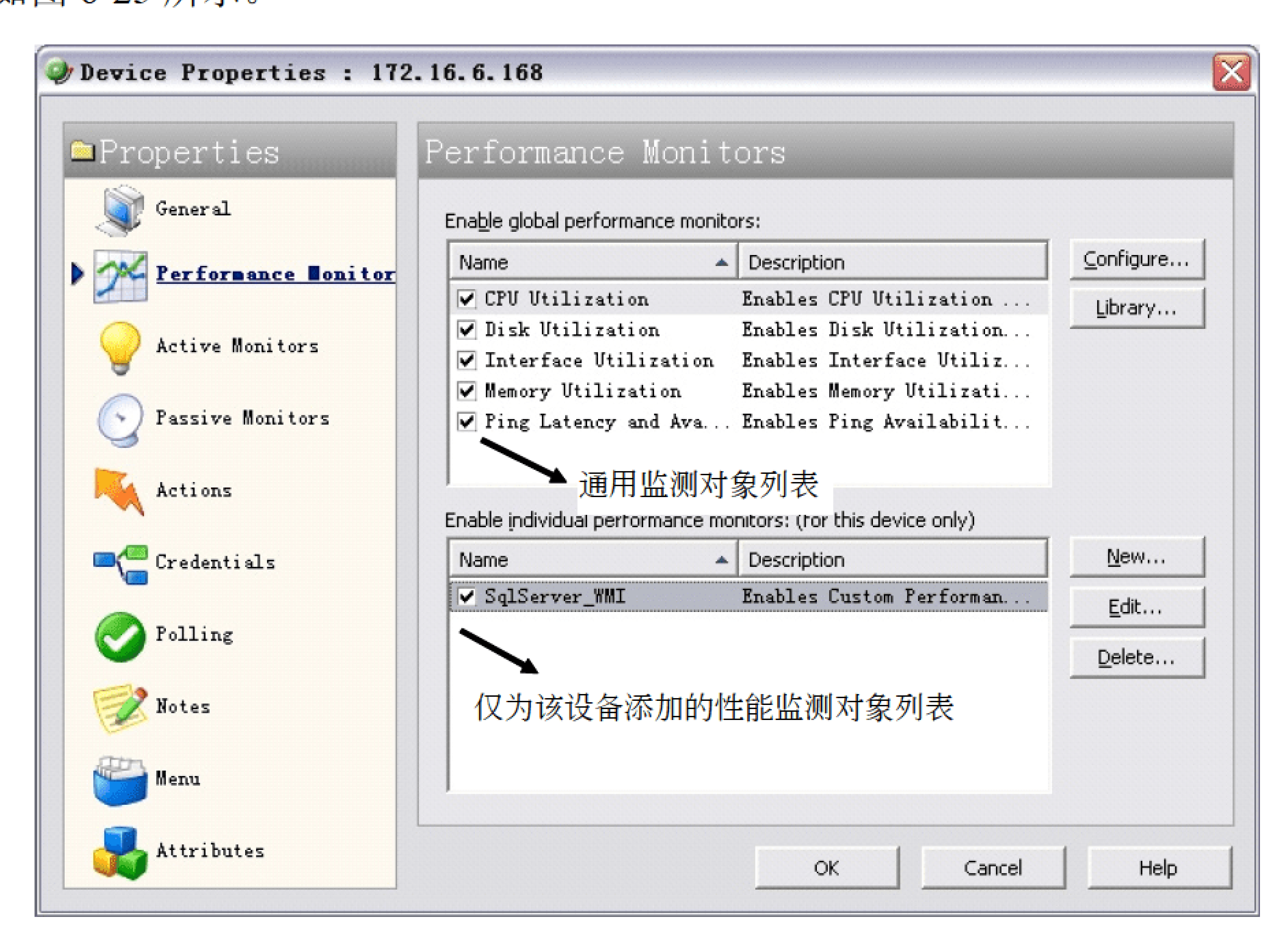


图 6-25　设备性能监视器属性

在性能监测中，如果监测对象是 Windows 或 Unix/Linux 系统的服务器，通过 SNMP 可获取 CPU 利用率、磁盘利用率、接口流量、内存利用率、Ping 操作响应时间及可用性；

如果监测对象是路由器/交换机等网络设备，能够采集其各个接口状态，如果网络设备有CPU或存储介质，则同样能够采集到其性能信息。

（2）WhatsUp Gold 要从 SNMP 设备上读取数据，必须获得被访问设备的许可，在为设备配置监控程序时，需要提供正确的 SNMP 访问设字符串，并与设备中事先设置的 Read Community String 相匹配，SNMP 才能正确访问设备。如果无法提供正确的字符串，程序将无法获取数据或使用指定的监控程序（注：SNMP 被动监测程序不需要证书）。

证书库中包含了 SNMP 证书，可从设备属性的 Credential 页面来选择，如图 6-26 所示。在后续的章节，将详细介绍证书的添加和修改。

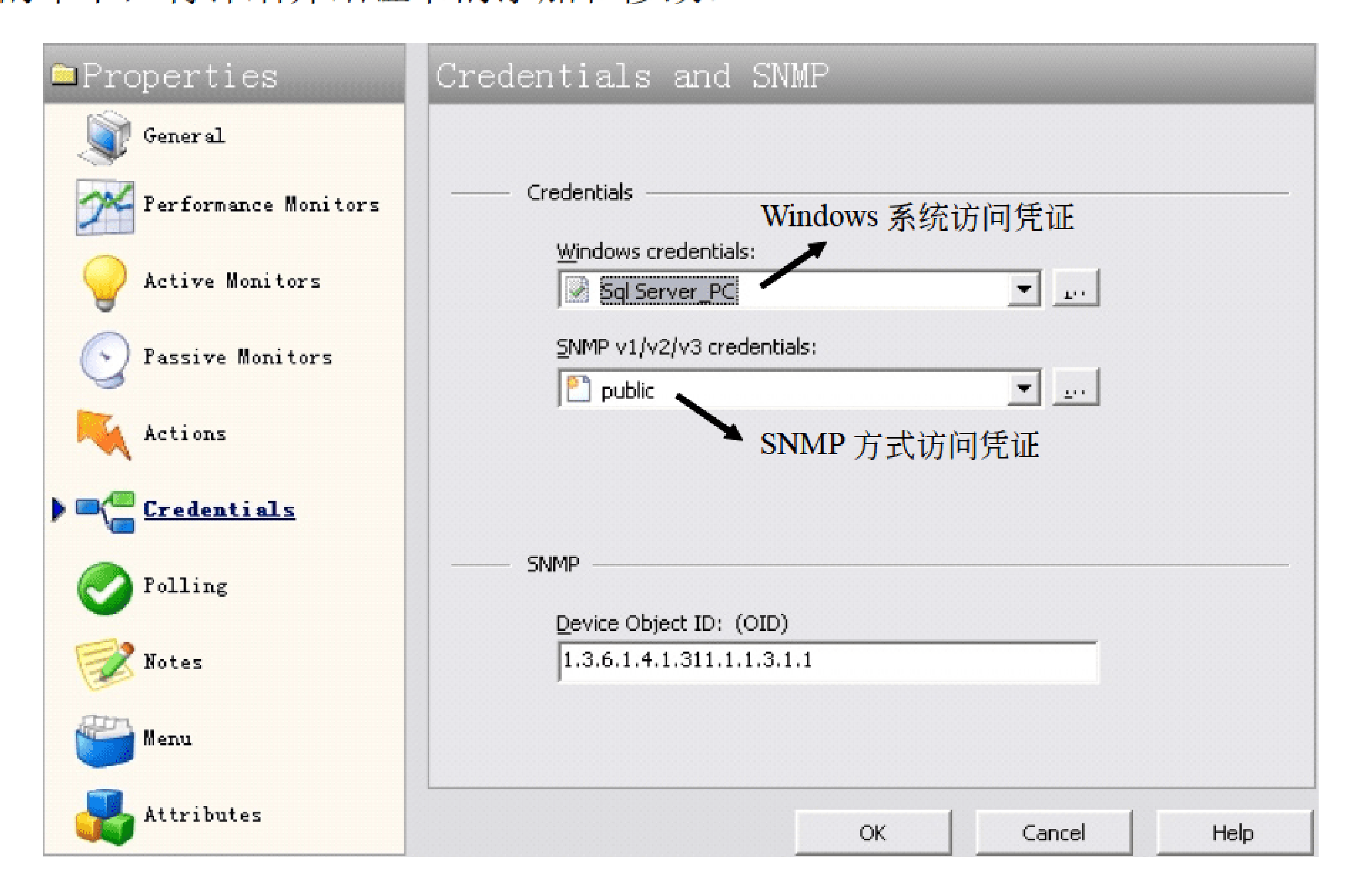


图 6-26　选择访问设备的认证字符串

选择正确的证书许可之后，双击性能监测项目，即可查看 CPU 利用率、磁盘利用率等信息，或者通过单击 Configure 按钮查看。

（3）在 Performance Monitor 界面中单击 Library 按钮，可配置性能监测项目库，在该界面中可对现有性能检测项目做更改或新增监测项目，如图 6-27 所示。

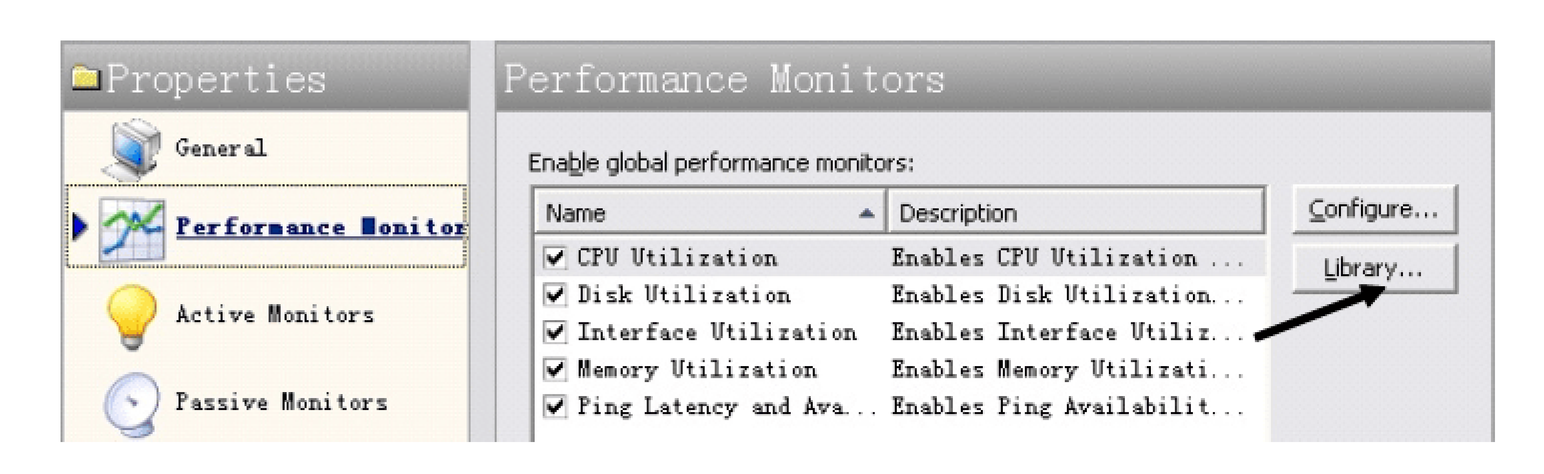


图 6-27　打开性能监测项目库

单击 Library 按钮后，将打开性能监测对象库的添加界面，如图 6-28 所示。

在图 6-28 中，性能监测库中允许添加 3 种类型的监测项目，包括基于脚本程序的性能监测 Active Script Performance Monitor、基于 SNMP 协议的性能监测 SNMP Performance Monitor 及基于 Windows 管理规范的性能监测 WMI Performance Monitor。通过这 3 种性能

监测类型，可以采集到设备更多的信息，例如采集 CPU 温度、内存进程数、应用程序占用内存等各种各样的设备信息。

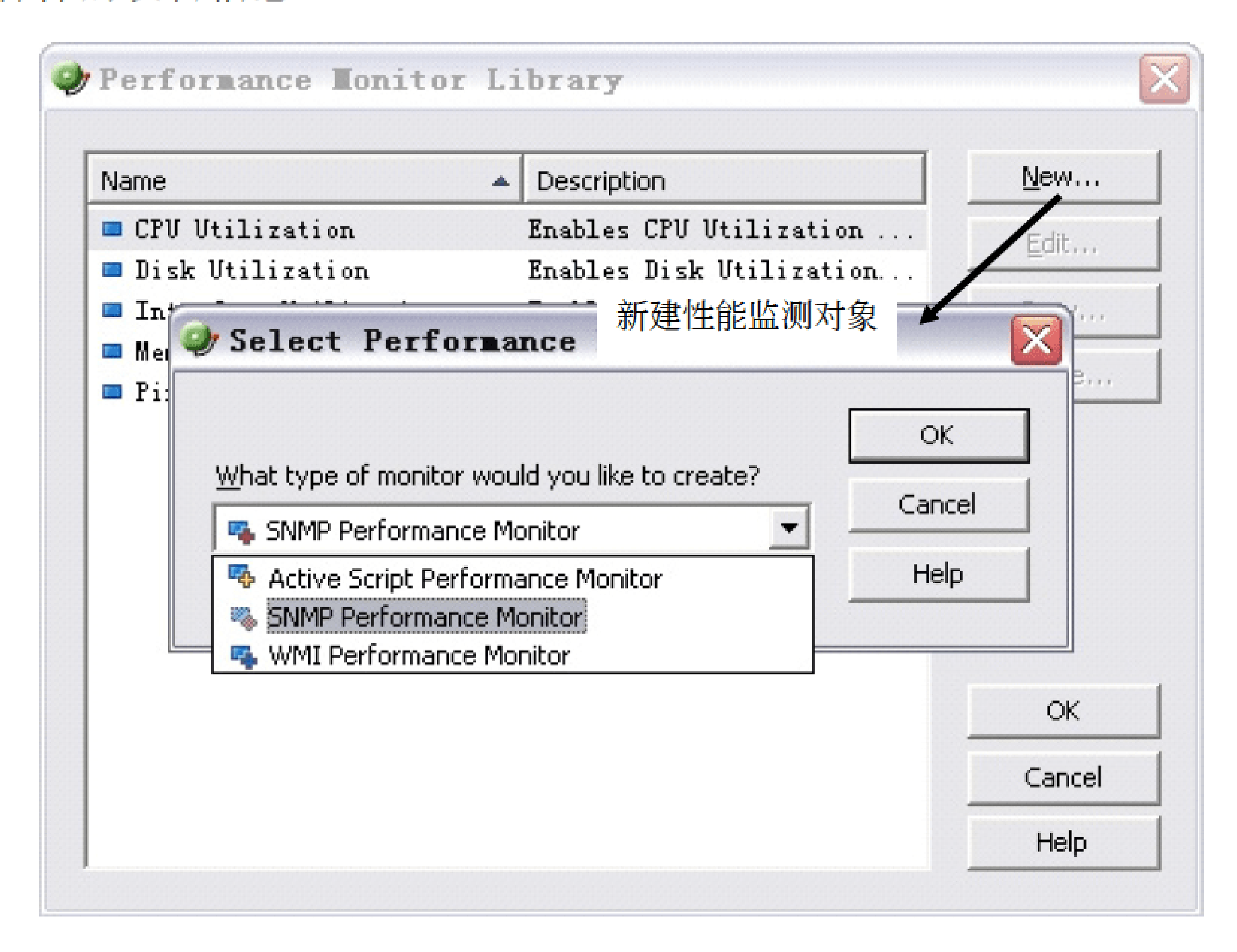


图 6-28　配置性能监测库

具体采集设备基础信息、添加 SNMP 监测内容、WMI 性能监测方式，将通过实例在第 7 章的扩展应用详细介绍。

注意：在该库中新增加的性能监测项目具有通用性，在其他设备的性能监测页面中新增的性能监测项目也将出现。

（4）如果仅针对当前设备添加其他性能监测项目，可在 Performance Monitor 界面下方 Enable individual performance monitors:（for this device only）区域，为该设备添加单独的性能监测项目。单击 New 按钮打开新建性能监测对象界面，如图 6-29 所示。该界面下新建的项目仅为该设备服务，不具备通用性。

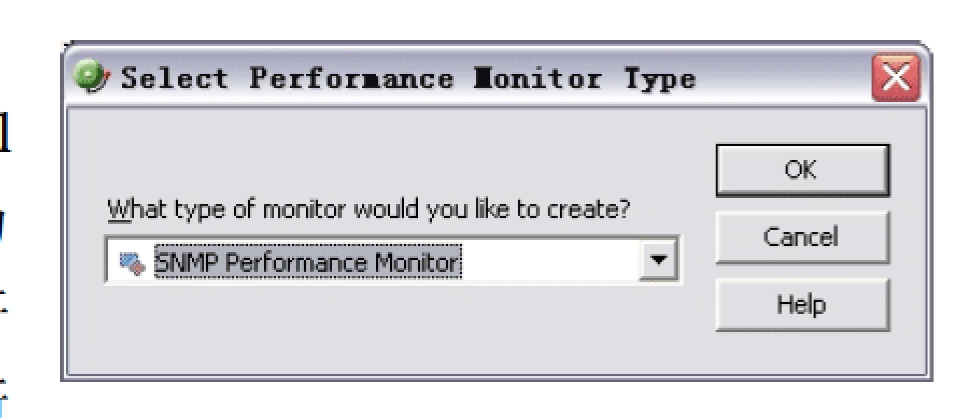


图 6-29　性能监测项目种类

6.2.4　Active Monitor 主动监测

WhatsUp Gold 按照轮询的时间间隔询问主动监测项目，访问设备上对应监测项目是否运行正常，并获取监测结果。

选择 Active Monitor 选项，在 Active Monitors Attached to this device 框中列出来了 WhatsUp 为该设备添加的主动监测项目，可以编辑已有项目或为该设备添加更多的主动监测项目。

1．添加主动监测项目

在最初查找设备时，通过 SNMP 扫描网络设备的过程中，SNMP 协议会根据选择的服务项目（Ping、HTTP、POP3 等）逐一“询问”设备是否提供该服务。如果设备提供相应的服务且运行正常，则会回应询问，并把回应的服务列入到主动监测项目中。例如，如图 6-30 中的设备在查询时，对 HTTP、Ping 和 SMTP 服务的询问做出了响应，于是这 3 项服务列入了主动监测的内容，如图 6-30 所示。

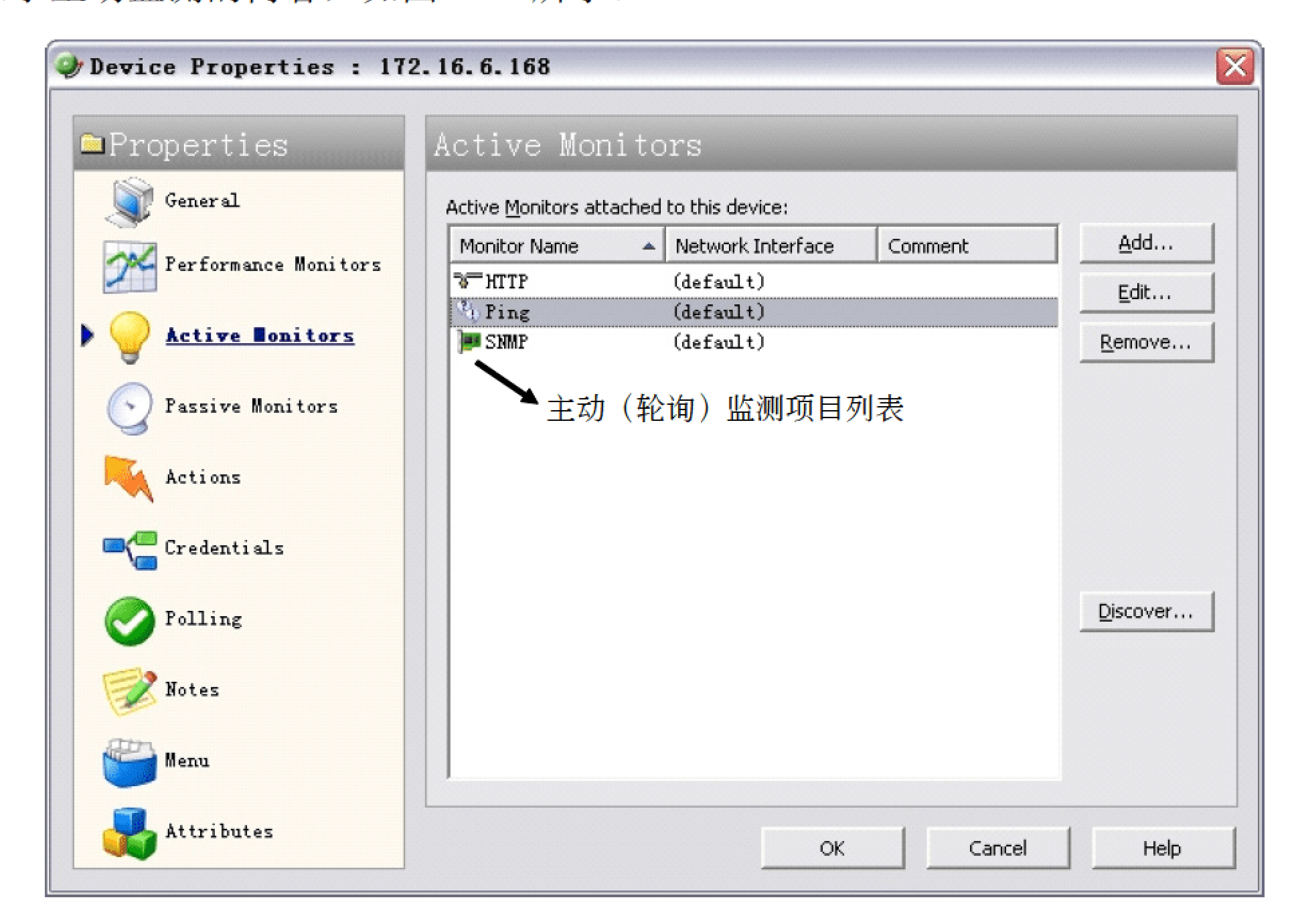


图 6-30　主动监测项目配置

（1）添加主动监测内容，也就是添加更多的轮询项目。单击图 6-30 中的 Add 按钮，弹出新增对话框，如图 6-31 所示。

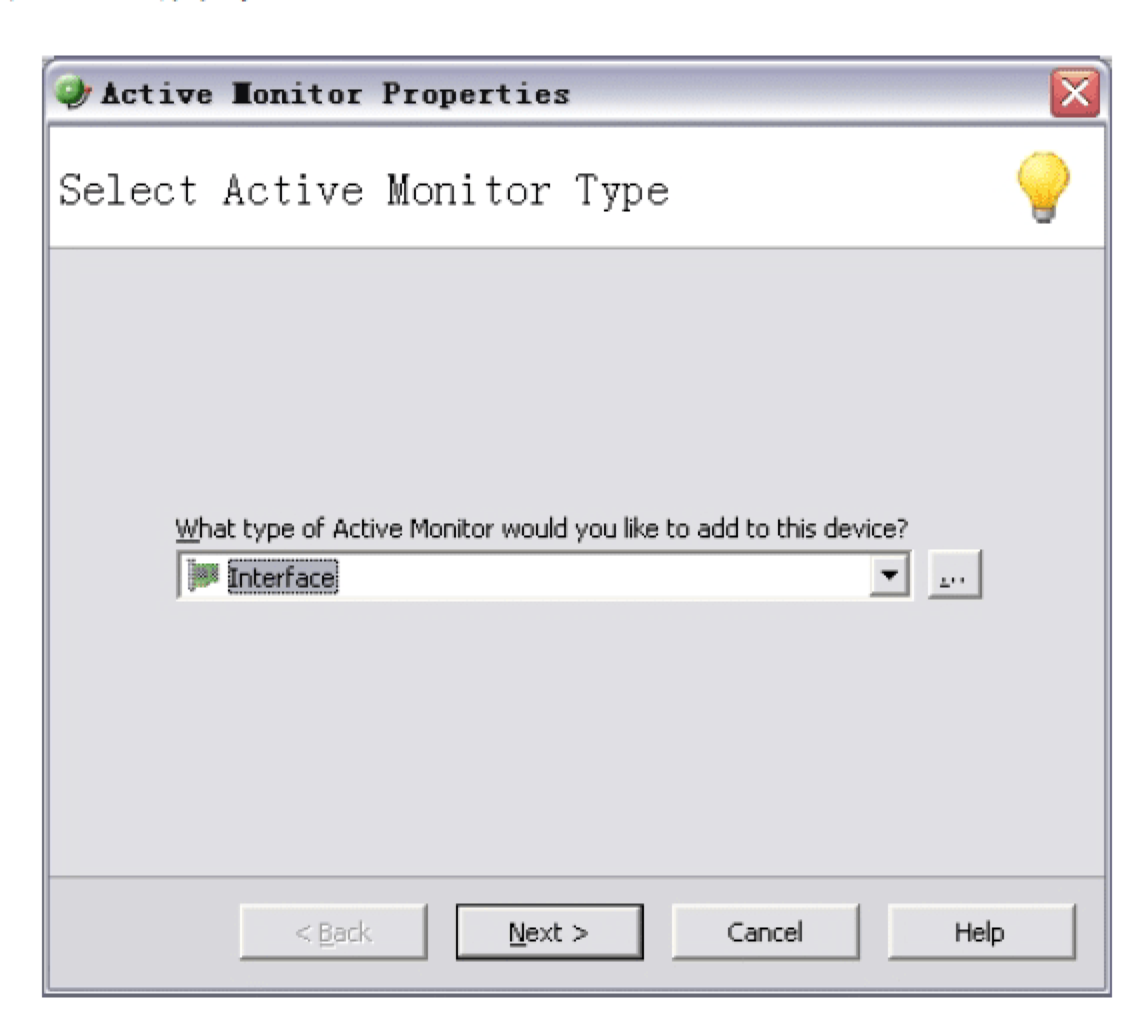


图 6-31　添加主动监测向导

（2）在图 6-30 中，选择主动监测类型下拉列表框，下拉列表中列出默认提供的常用主动监测项目（如图 6-32 所示），可在列表中选择需要监测的项目。

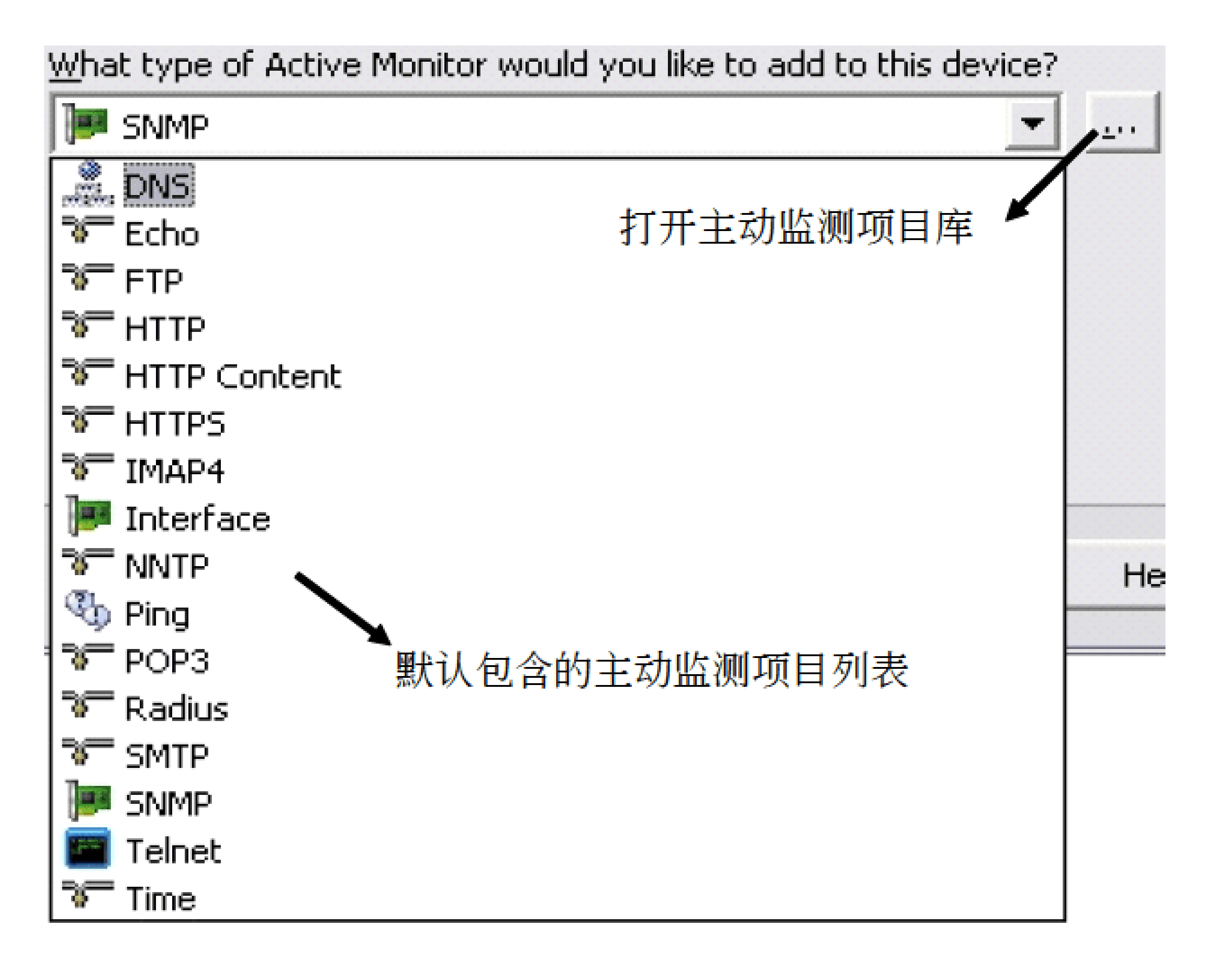


图 6-32　常用主动监测项目类型

（3）如果需要添加非常用监测项目（例如 SQL Server 监测、Exchange Server 监测）等，则单击下拉列表框右侧的浏览按钮，打开主动监测库。其中包含了所有 WhatsUp Gold 支持的主动监测类型，可对已存在项目进行更改和添加其他扩展监测项目，如图 6-33 所示。

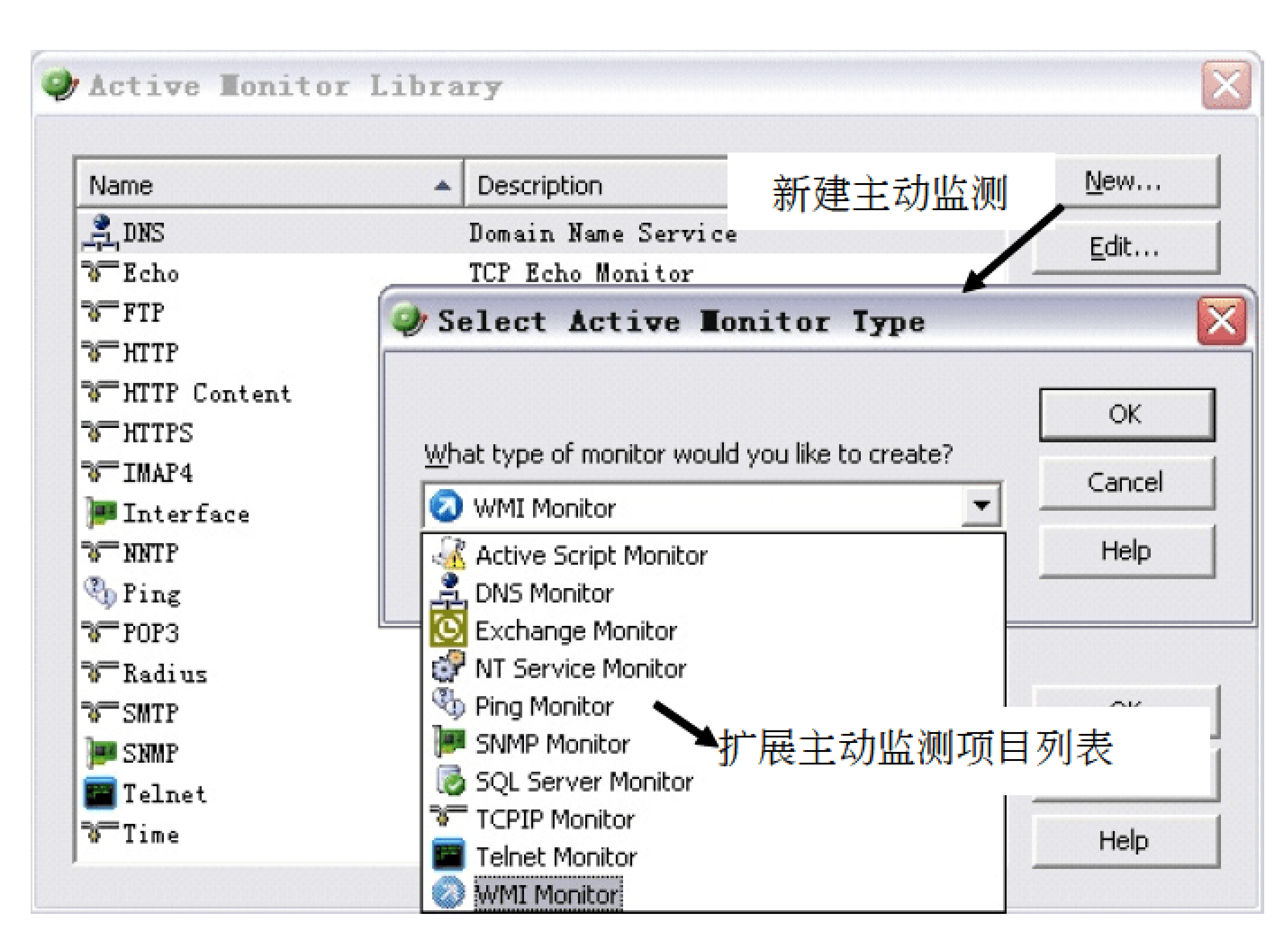


图 6-33　扩展主动监测项目类型

在 6.1.1 节中，已经详细列出了主动监测常用的监测项目，此处不再重复。在表 6.4 中列出了可增加的扩展主动监测类型，用于可实现对邮件服务器各项服务的监控、SQL 数据库性能监测及 Windows 系统各项性能的监测。

（4）添加扩展的监测项目还需要做额外的设置，将在后续章节进行讲解。此处主要介绍主动监测的添加过程。选择添加列表中默认包含的对象 HTTP 后，单击下一步按钮，打

开接口选择界面，选择默认的监测接口即可，如图 6-34 所示。如果设备包含多个网卡接口，则从下拉列表中选择要监测的网卡。

表 6.4　扩展主动监测类型

序号	类型	监测对象及描述
1	Active Script Monitor	通过编写并执行 VBScript 或 JScript 脚本来监测对象。如果运行脚本后返回错误代码，则认为该监测对象是停止的
2	Exchange Monitor	包括对 Exchange 邮件服务器性能阈值监测及 Exchange 提供的服务监测
3	NT Service Monitor	监测 Windows 主机所提供的某项服务的状态，并尝试去重启服务器（如果获得超级用户的权限）
4	MSSQLSERVER	包括对 MS SQL Server 数据库服务器性能阈值监测及 MS SQL Server 提供的服务监测
5	WMI Monitor	监测 Windows 系统中任何性能计数器数值，当数值发生变化或超出某区间或者出现数值异常波动等情况下触发报警

（5）选择接口后，进入报警提示动作设置界面（如图 6-35 所示），当监测的对象状态变化时将触发所选择的报警提示动作，也可选择不执行任何报警动作。完成该步骤之后，即完成了主动监测的添加（报警提示动作的详细介绍请参照 6.3 节）。

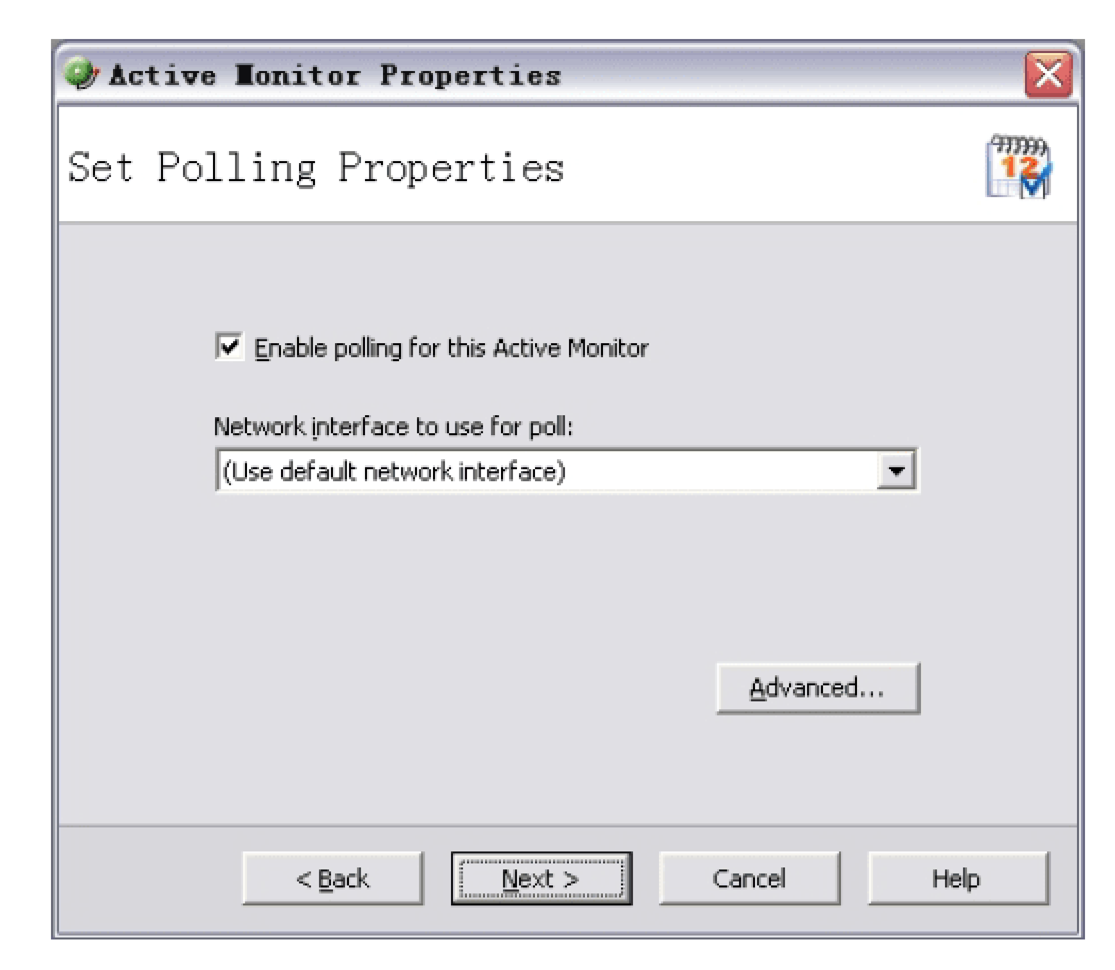


图 6-34　添加主动监测——选择接口

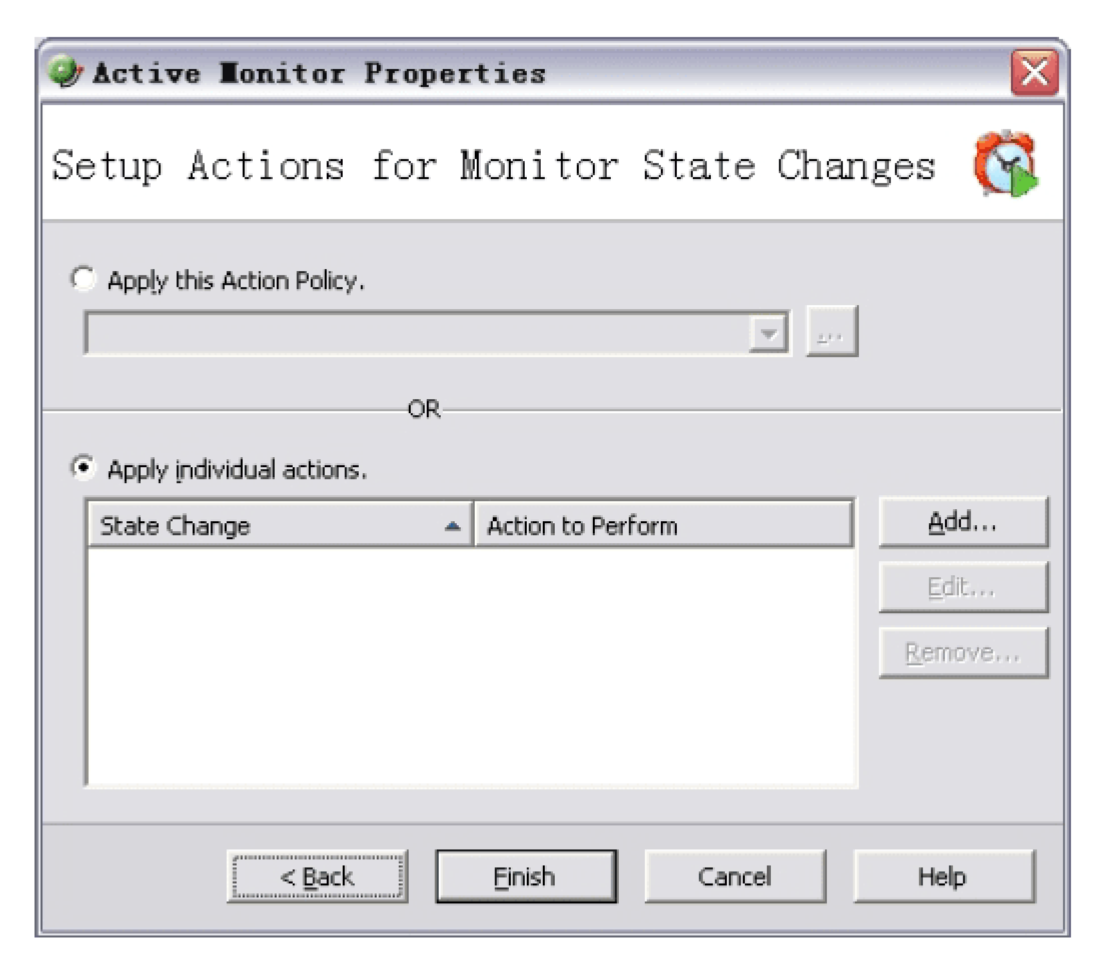


图 6-35　添加主动监测——选择提示动作

2. 编辑主动监测项目

在主动监测界面选择已有的监测项目，并单击 Edit 按钮，可编辑该监测项目的轮询和报警提示动作，如图 6-36 和图 6-37 所示。

6.2.5　Passive Monitor 被动监测项目

被动监测 Passive Monitors 项目监听从设备发出的信息，并通知 WhatsUp Gold 信息内容。其效率比对监测项目逐一做轮询更高，监听项目能够监听网络传输状态及应用程序的事件。

选择设备属性界面的 Passive Monitors 页面，在该页面中列出了针对所选设备的被动监

测项目，并能对监测项目做新增、修改和删除操作，如图 6-38 所示。

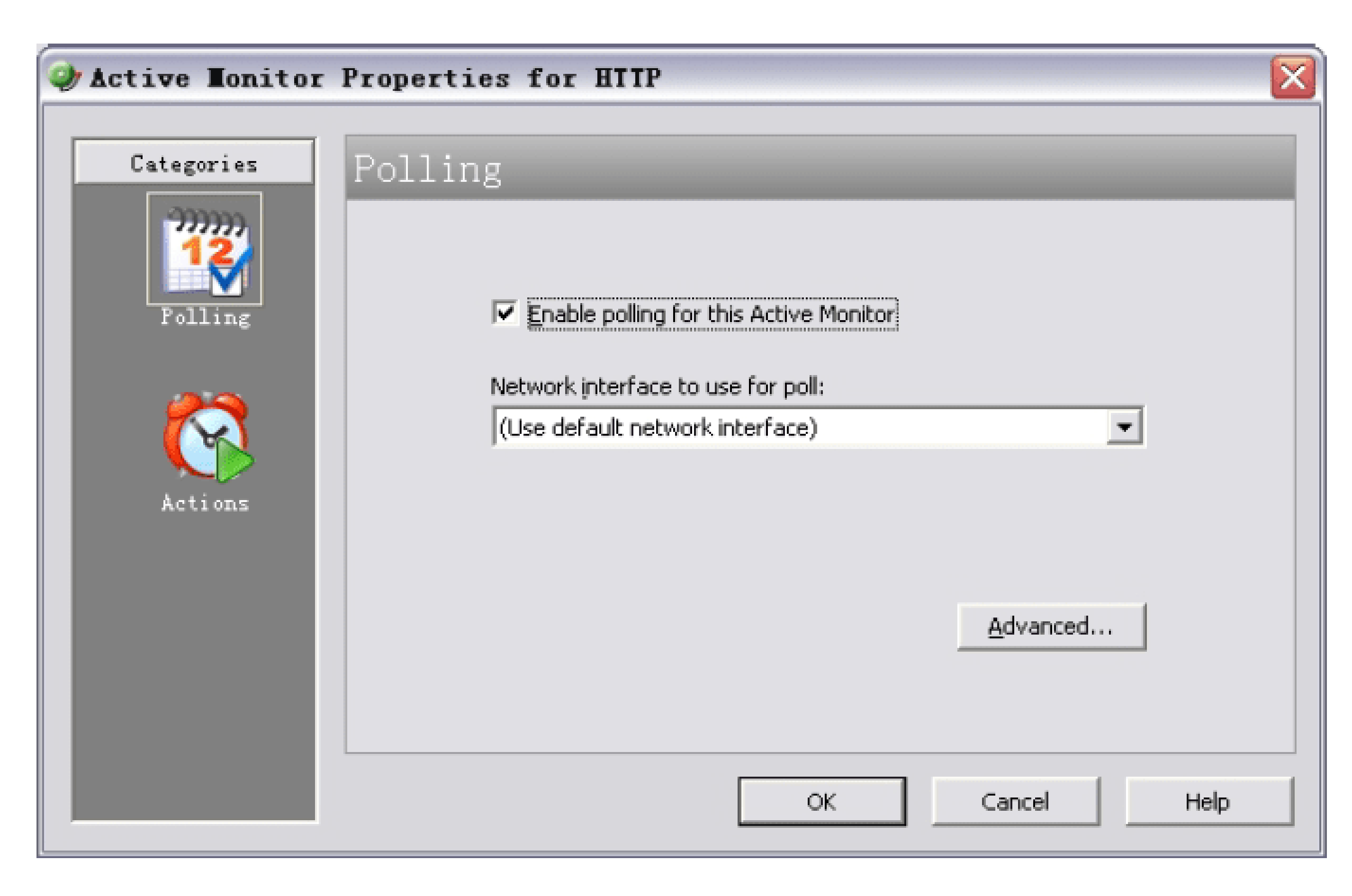


图 6-36　主动监测——设置轮询的网卡接口地址

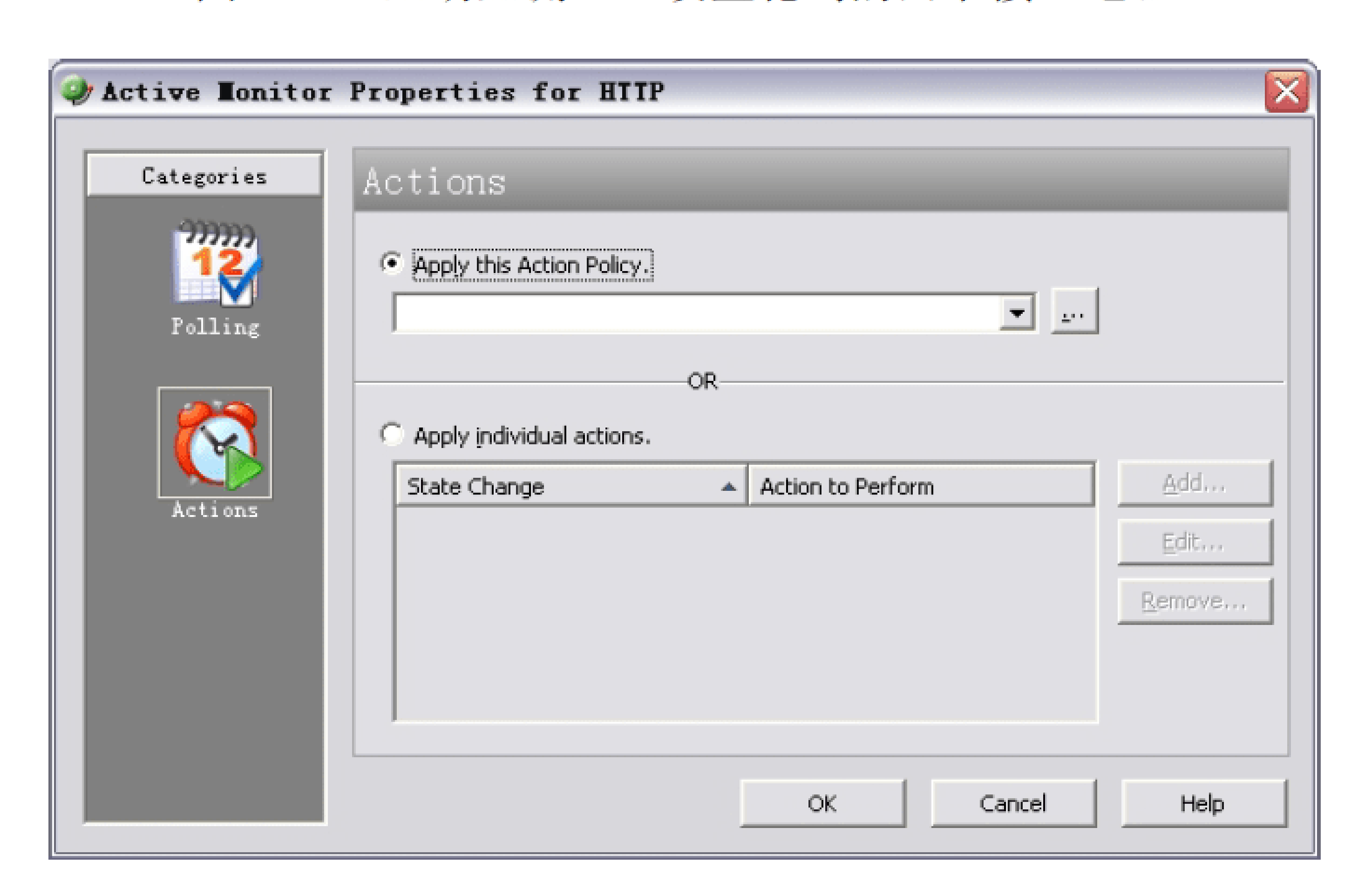


图 6-37　主动监测——为该监测项目添加提示动作

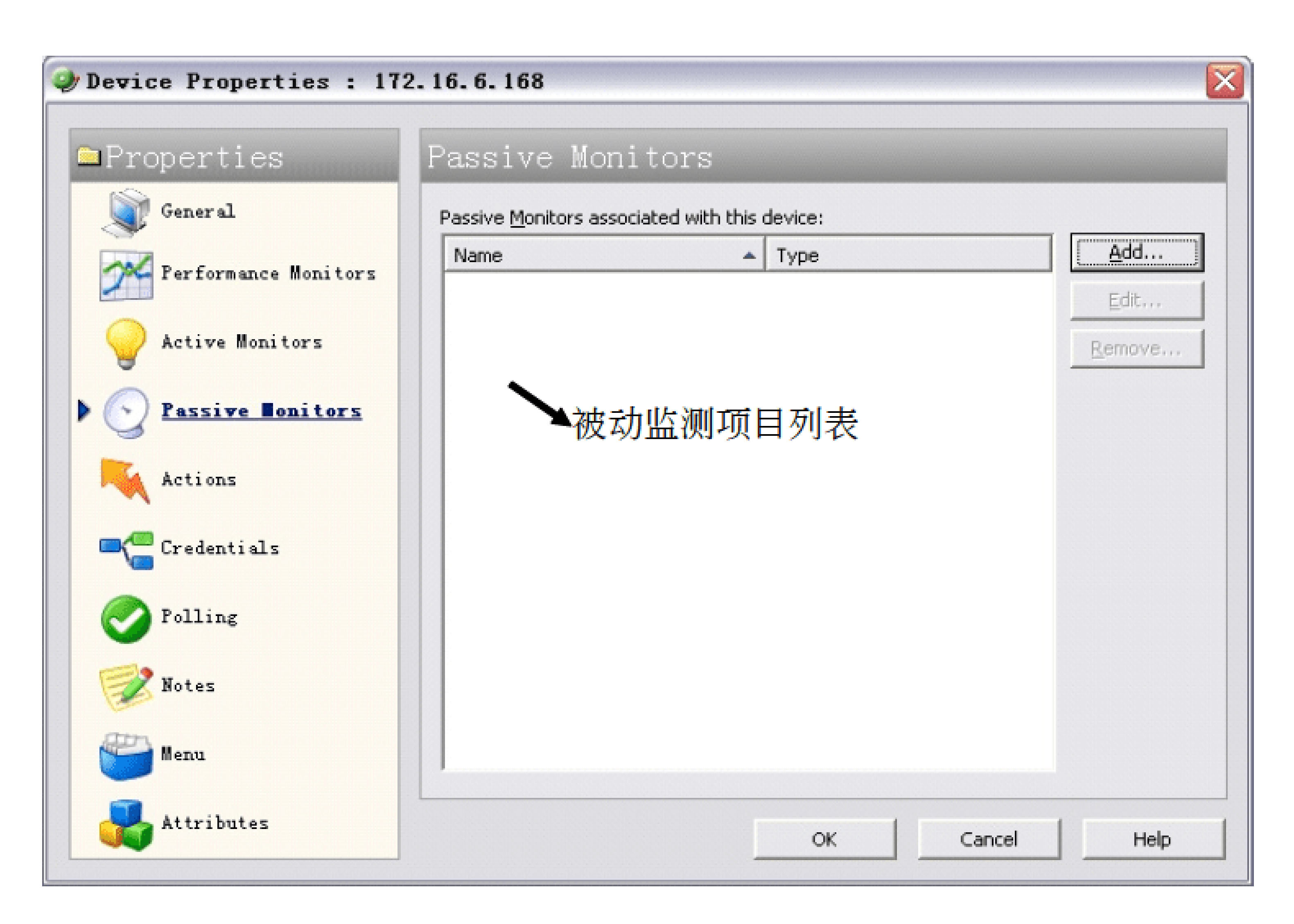


图 6-38　被动监测项目配置

1．3 种被动监测类型介绍

SNMP Trap（SNMP 陷阱信息）：该类信息为非请求类信息，由设备主动发出以提示设备状态的改变，例如路由器某端口关闭、打印机缺纸等消息。

Syslog（系统日志）：系统日志监听 UDP 端口 514，接收从网络设备发出的标准 UDP 消息，以实现对日志信息的监测。该信息是由设备发出的日志记录中某段特殊记录或者记录中的某段文字构成。通常，日志信息从 Unix 系统中发出，但也能够从非 Unix 系统中发出。日志信息中可能包含任何系统信息，例如设备停机或者试图登录到操作系统中的访问等。

WhatsUp Gold 记录系统日志成为单独的文件，并记录时间戳和发出日志的 IP 地址，并每周递增的存储这些数据为一个文件。文件名命名格式为 SL-YYYY-MM-DD.tab。

Windows Event Log（Windows 系统事件日志监测）：该监测项目能够监测 Windows 服务的启动或停止、登录 Windows 失败或者其他 Windows 实体中的事件日志。

注意：当某设备添加被动监测项目后，则该设备图标左上方增加了方框，显示为；当监测发现未能识别的设备状态改变时，图标左上方方框将改变颜色，显示为；当改变的状态被识别认可后，左上方又恢复为空白方框图标。

2．配置监听程序

在添加被动监测项目之前，需对监听机制做配置。选择主界面的菜单中的 Configure | Program Options 命令，并选择 Passive Monitor Listeners 选项页（如图 6-39 所示），该页面中可对 3 种被动监测方式做配置如下。

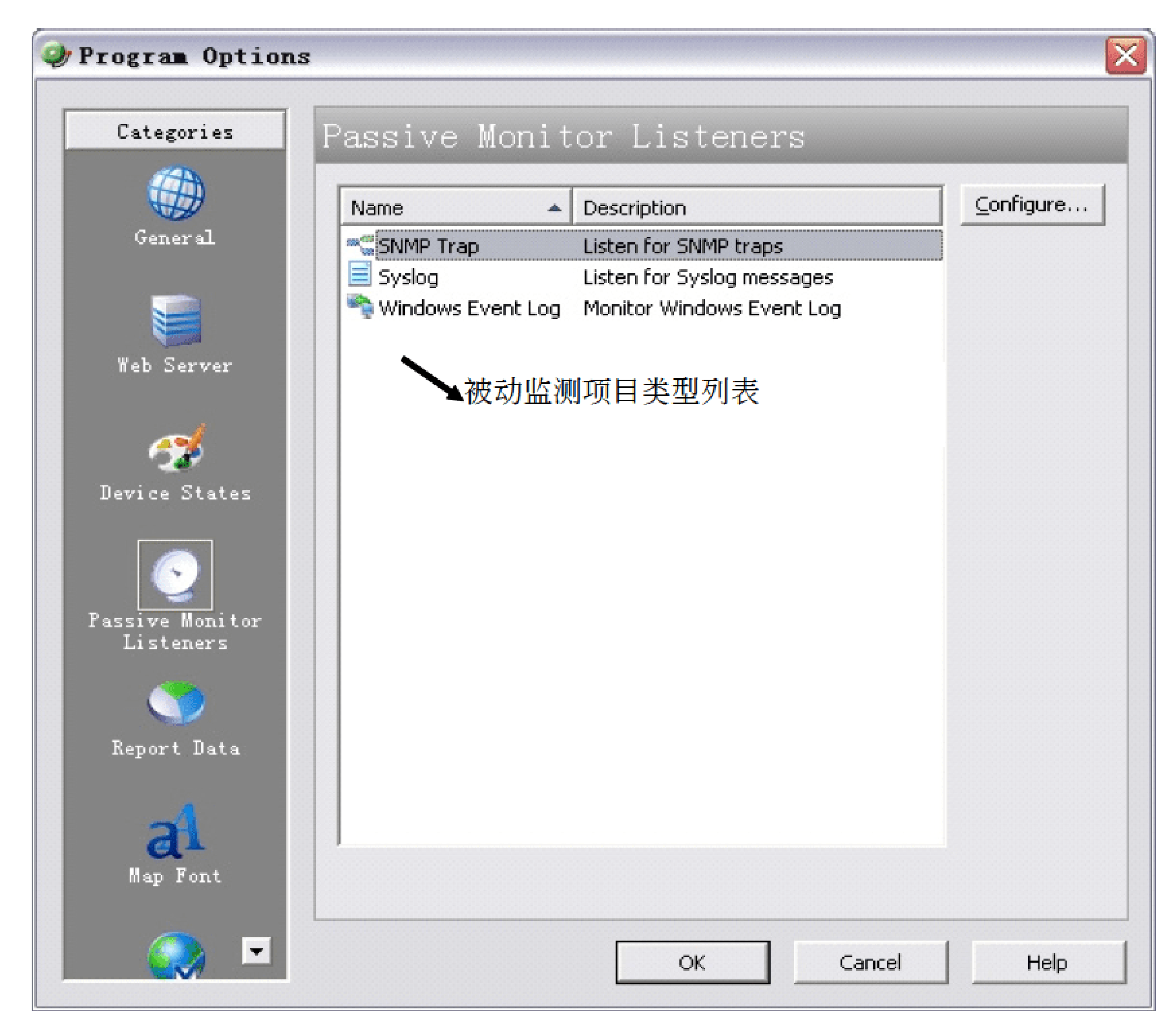


图 6-39　被动监听属性配置

（1）在列表中选择 SNMP Trap 选项，并单击 Configure 按钮，打开 Trap 项目配置界面，如图 6-40 所示。

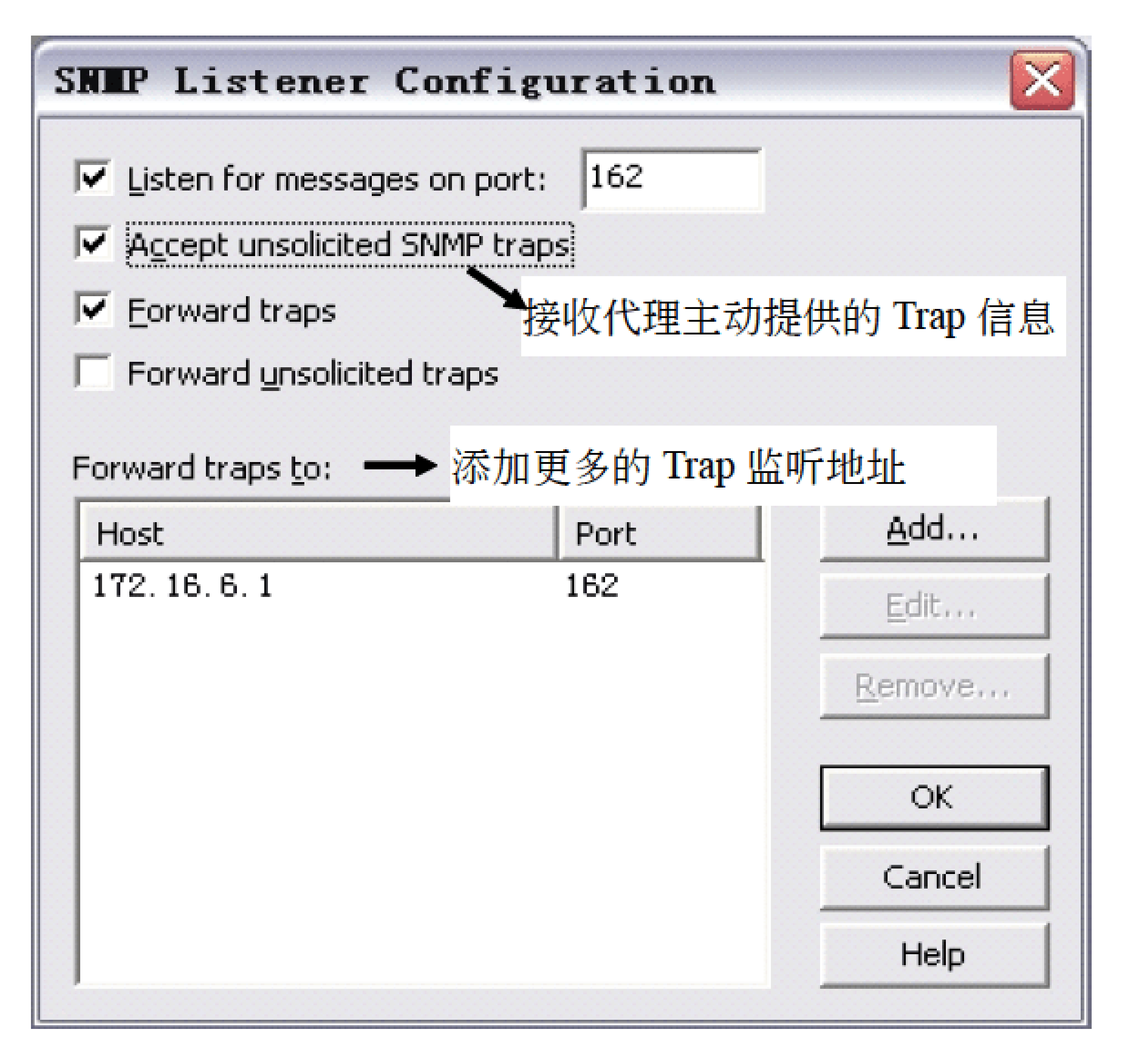


图 6-40　SNMP Trap 设置

在 SNMP Trap 设置界面，可选择监听的端口，默认的监听端口是 162，较为常用的端口还有 5000，该端口也就是监测设备发送 Trap 信息所设置的端口。设置是否监听 SNMP 主动提供的 Trap 信息，以及添加更多的 Trap 监听选项。

（2）选择 Syslog 选项，并单击 Configure 按钮，打开 Syslog 监听项目配置窗口，如图 6-41 所示。

在 Syslog 设置界面，需要选择监听日志信息的端口，以及选择是否监听接收设备的日志信息。将选项选中才能够启动监听程序，监听默认 514 端口。

（3）选择 Windows Event Log 选项，并单击 Configure 按钮，打开 Windows 事件日志监听配置界面，如图 6-42 所示。

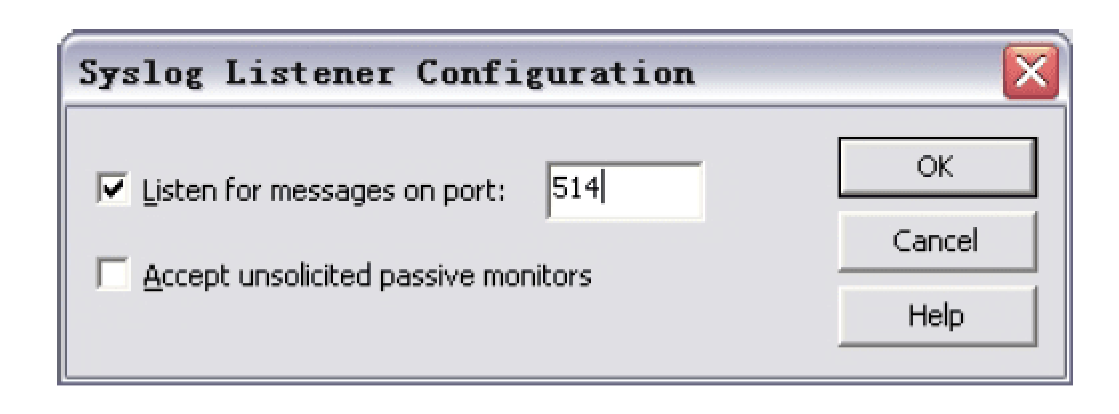


图 6-41　Syslog 设置

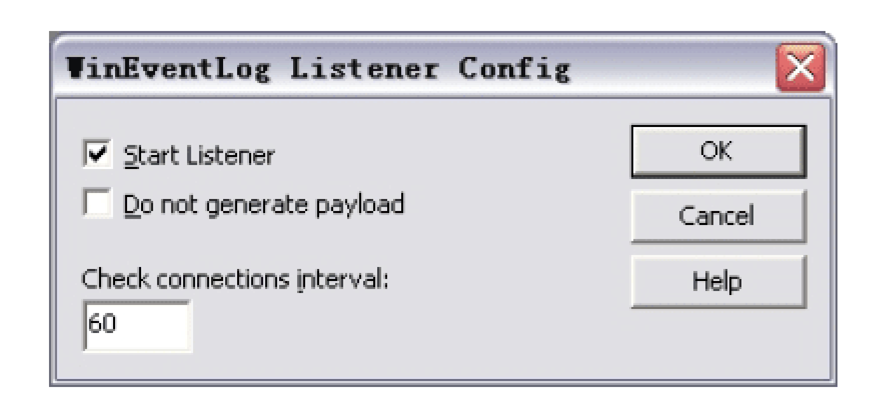


图 6-42　Windows Event Log 设置

注意：如果在安装了 WhatsUp Gold 程序的 Windows 主机上的“服务”中开启了 SNMP Trap 服务，那么需要停止该服务，以防止与 WhatsUp Gold 监听程序发生冲突。

3．添加被动监测项目

（1）设置完 Passive Monitor 属性之后，回到设备属性的 Passive Monitors 页面，为所选

设备添加被动监测项目，单击 New 按钮，打开新建界面，如图 6-43 所示。

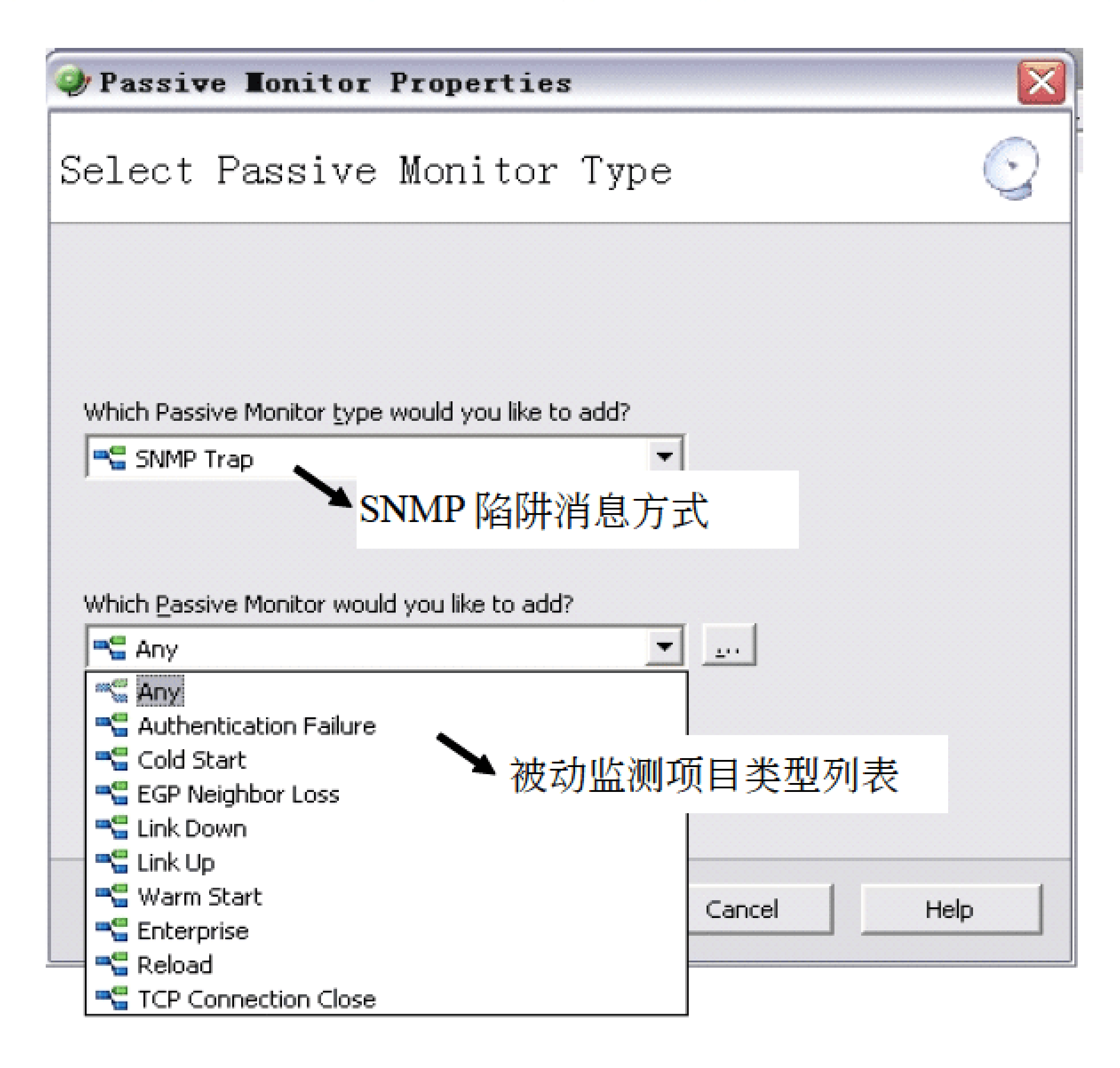


图 6-43　新建被动监测项目添加

（2）在新建界面中，列出了被动监测项目类型及每个类型下的监测项目细目。如果选择监测类型为 SNMP Trap，则有较多的细目选项，SNMP Trap 监测类型细目描述见表 6.5。

表 6.5　SNMP Trap 监测类型细目

序号	类　型	监测对象及描述
1	Any	任何监测类型
2	Authentication Failure	登录认证失败
3	Cold Start	冷启动开始
4	EGP Neighbor Loss	外部网关协议发现邻居设备丢失
5	Link Down	设备端口关闭
6	Link UP	设备端口开启
7	Warm Start	热启动开始
8	Reload	重新加载程序
9	TCP Connection Close	TCP 传输控制协议关闭

如果选择类型为 Syslog 或 Windows Event Log，则细目可选项只有 Any，即接收任何类型的系统日志信息和任何类型的应用程序时间日志，如图 6-44 所示。

（3）选择类型及监测具体项目后，需要为该监测项目添加报警提示动作，如图 6-45 所示。此处在下拉列表中选择 Sound-Down5，即当监听到系统关闭或无法连接超过 5 分钟时，WhatsUp Gold 发出声音报警提示。

注意：在图 6-45 的 Blackout Schedule 中可设置不接收的监听信息的日程。

（4）添加 Action 后即完成了被动监测项目的添加。在被动监测项目列表中列出了新增加的项目，如图 6-46 所示。

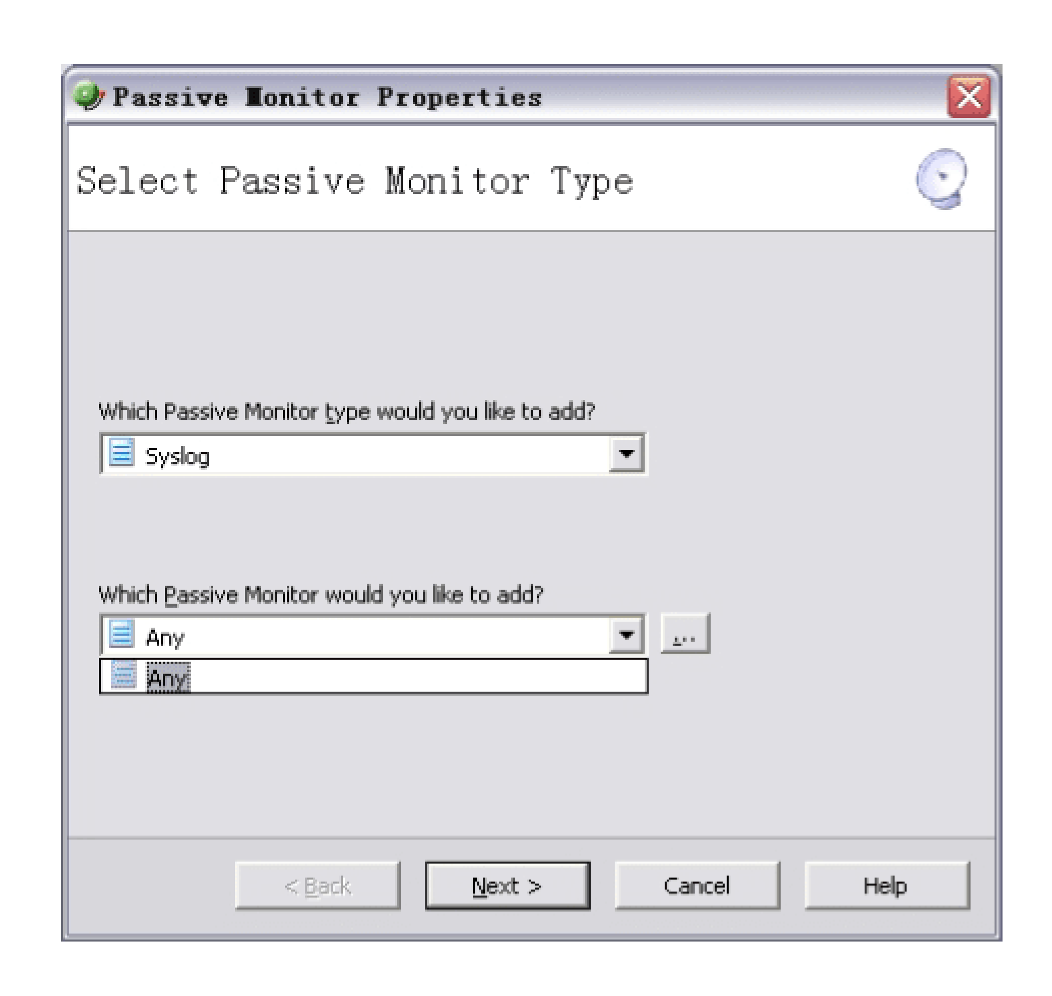


图 6-44　被动监测类型和细目选择

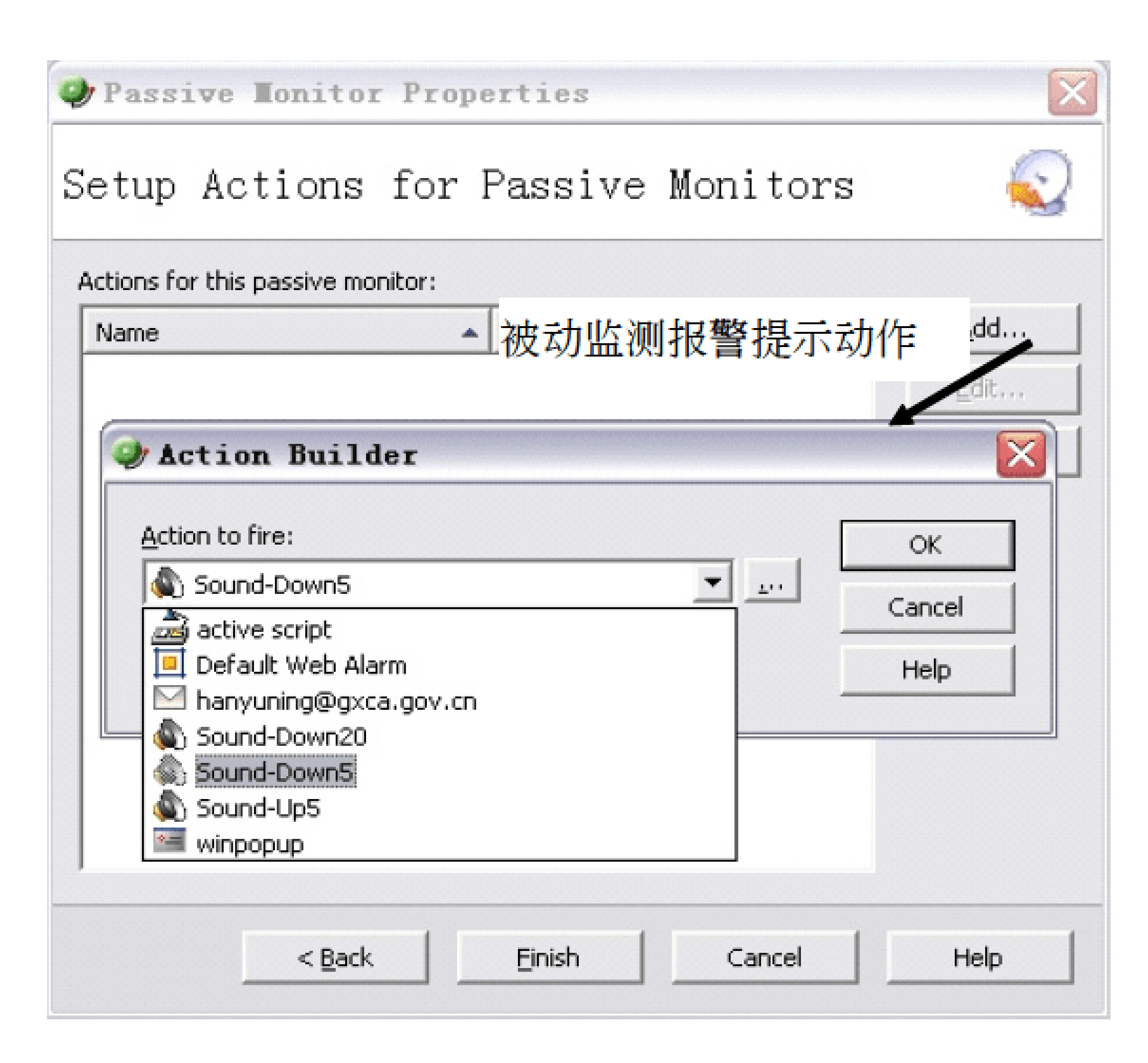


图 6-45　为被动监测项目添加报警动作



图 6-46　被动监测项目列表

6.2.6 Actions 报警提示动作

在 Actions 属性中有两个概念，即 Action 和 Action Policy 需要区分。Action 是触发的单一动作，例如某时刻发出声音、发送一封电子邮件、弹出提示框等。Action Policy 则是

几种动作的组合，例如系统停止运行时触发报警动作，发出声音报警同时发出电子邮件信息，在系统恢复启动时又触发声音告警等，它是一系列动作的组合。

单一报警动作保持于动作库 Action Library 中，而动作组合的策略保存在策略库中，选择报警动作的操作如下：

选择设备属性界面中的 Actions 页面，打开报警提示动作配置界面，如图 6-47 所示。

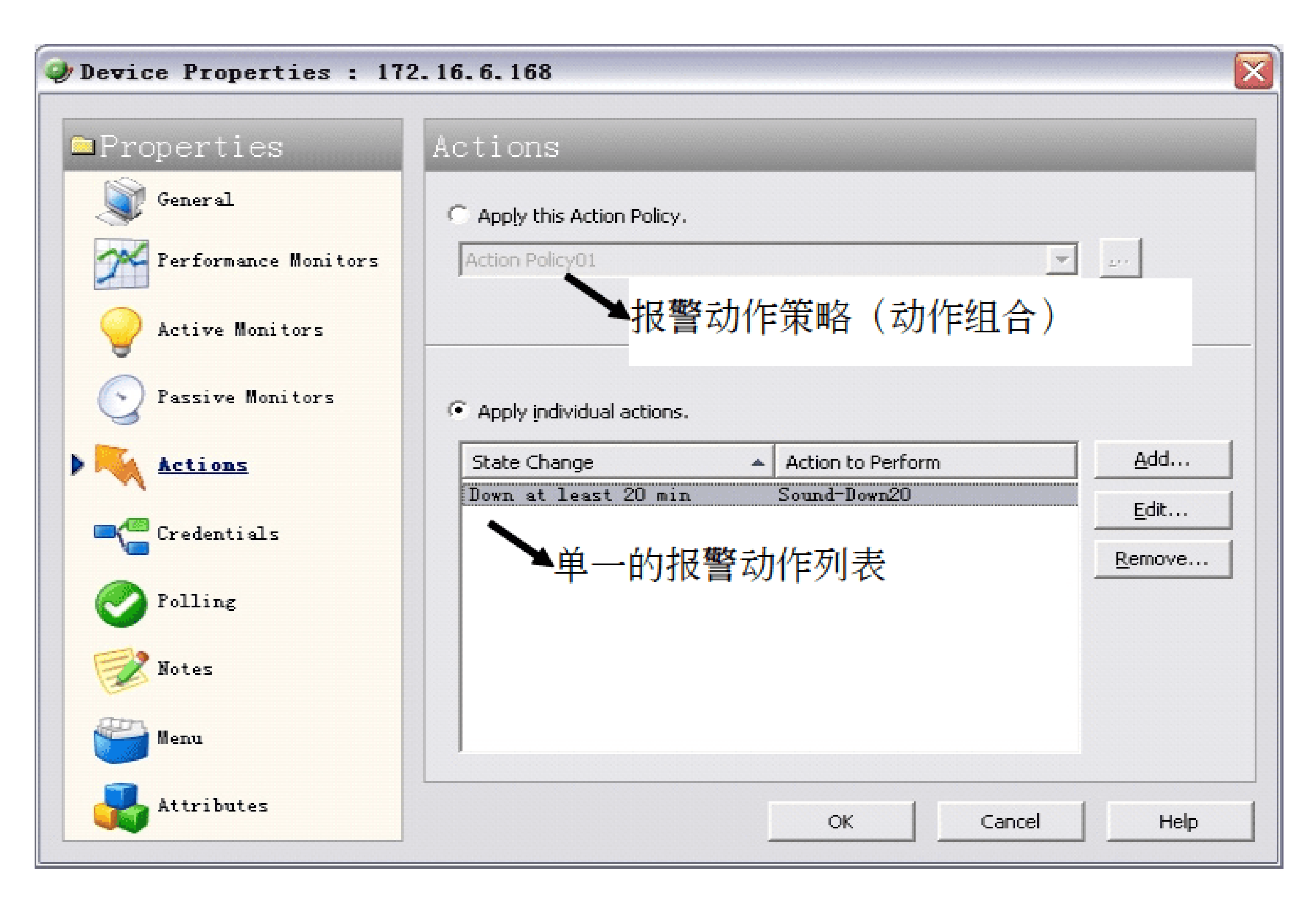


图 6-47　报警动作配置

在 Actions 界面上方，选中 Apply This Action Policy 复选框，可从策略库中选择已经配置的报警策略选项，则对应的策略应用到该设备上。当 WhatsUp Gold 对设备做轮询，发现设备无应答时，则会触发执行 Action Policy 策略中配置的提示动作。

单击下拉列表右边的浏览按钮【…】，可打开动作库配置界面。在动作库中添加的单个动作可添加到某策略中，也可在其他配置动作界面进行调用。

该界面右上方的 Action Policy 策略为通用提示动作，可应用于各个设备，但界面下方的列表显示框中的动作列表仅应用于所选设备，可为该设备添加自定义的个别报警提示动作或者几个动作，具体添加操作在 6.3 节进行详细介绍。

注意：（1）在该 Actions 页面配置的报警提示动作，是针对该设备状态改变（由 Up 变为 Down，或者由 Down 变为 Up 两种）所作出的提示动作，为设备级的告警。也可以在主动监测和被动监测页面，针对该设备的各项服务（HTTP、FTP、SMTP 等）设置业务级别的告警。

（2）在某 Action Policy 策略中包含了几个提示动作，如果对其中某个动作进行删除或修改操作，那么已启用了该策略的设备。相应地，其中包含的动作也将被删除或更改。

6.2.7　Windows/SNMP Credentials 凭证

WhatsUp Gold 支持 SNMP v1、SNMP v2 和 SNMP v3 三个版本，v1 和 v2 版本在应用

程序与设备连接方式上非常相似，且同采用社区字符串安全认证机制。SNMP v3 提供和 v2 版本一样的数据，但是使用不同的认证方案来代替社区字符串安全机制。v3 版本在对设备做轮询时，要求登录用户名和密码。另外，用户可以配置 SNMP v3 设备在数据包发送到设备之前做加密处理。

1．凭证种类介绍

在设备属性界面选择 Credentials 页面，即可配置所选设备的访问凭证，如图 6-48 所示。

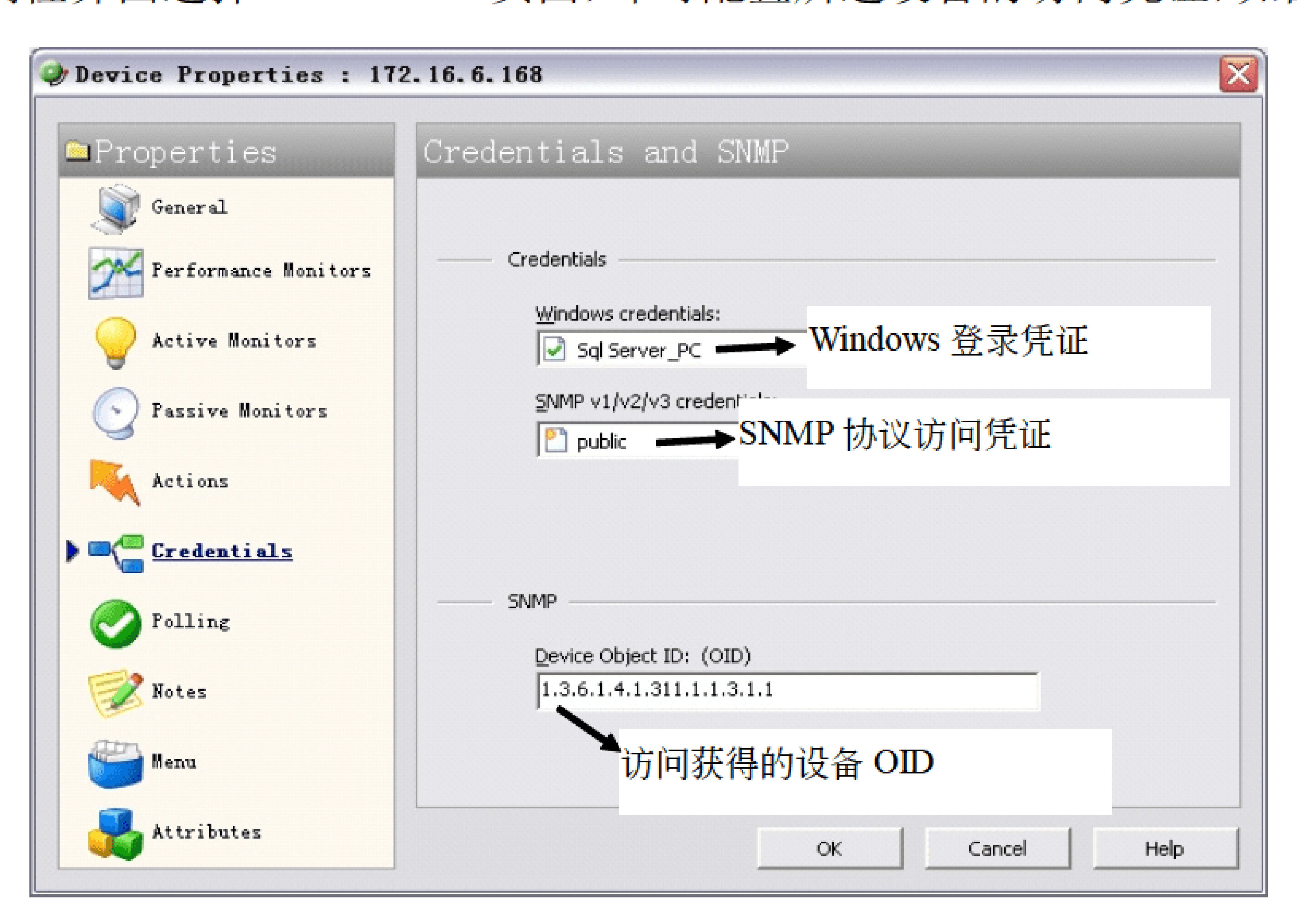


图 6-48　访问设备凭证配置

如果设备为 SNMP 协议管理的设备，则在 Map 视图中设备图标为 。

凭证包括 Windows 和 SNMP 两类。

Windows Credentials：选择登录 Windows 操作系统的账户和密码信息凭证，单击下拉列表右侧的浏览按钮，可对 Windows 凭证做新增、删除、修改等操作。

SNMP v1/v2/v3 Credentials：通过 SNMP 方式发现设备时，就需要用正确的 SNMP 凭证访问。如果社区字符串正确，该设备将记录正确的字符串，该界面 SNMP v1/v2/v3 Credentials 选项中也会自动显示正确的凭证。如果设备是通过其他方式扫描发现的，那么还需要单独为其配置访问凭证，供其他主动监测和性能监测的对象使用。单击下拉列表右侧的浏览按钮，可对凭证做新增、删除、修改等操作。

Device Object ID（OID）选项：OID 为 SNMP 管理对象标识，如果设备 SNMP 协议正常启用，则能够获取该标识数值。

2．添加 SNMP 凭证

Windows 凭证的添加在 6.1.1 节已介绍过。此处介绍 SNMP 类别凭证的添加。打开 Credentials Library 界面，单击 New 按钮新建 SNMP 类别凭证，如图 6-49 所示。

在类型下拉列表中选择 SNMP v1，如果被访问设备的社区字符串已经更改了默认值，则需要在 SNMP read community 和 SNMP write community 文本框中输入为该设备自定义的

访问字符串。为该凭证命名后，则在凭证库中建立了凭证，如图 6-50 所示。同样，可以在该界面中建立 Windows 访问凭证。

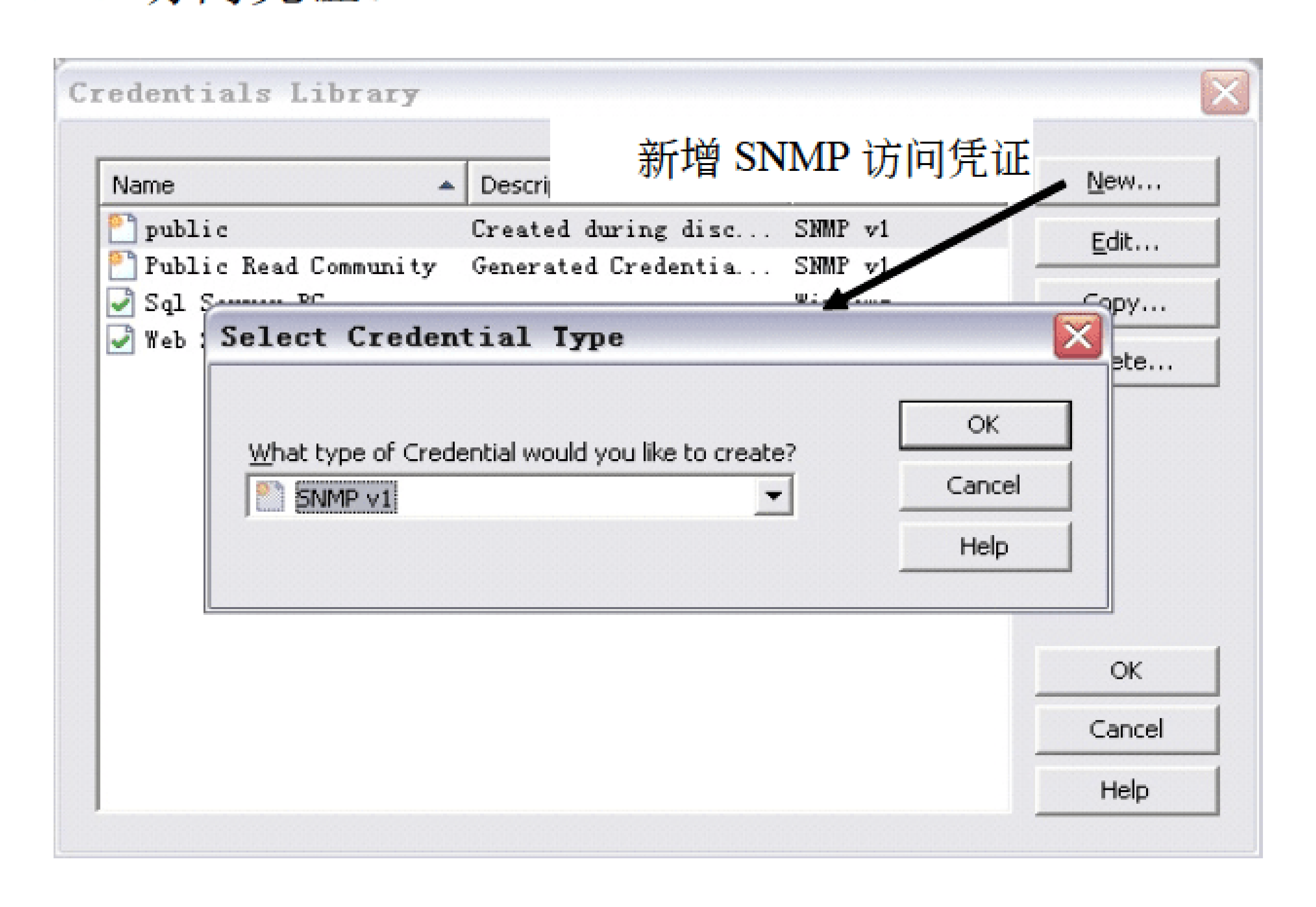


图 6-49　新增 SNMP 访问凭证

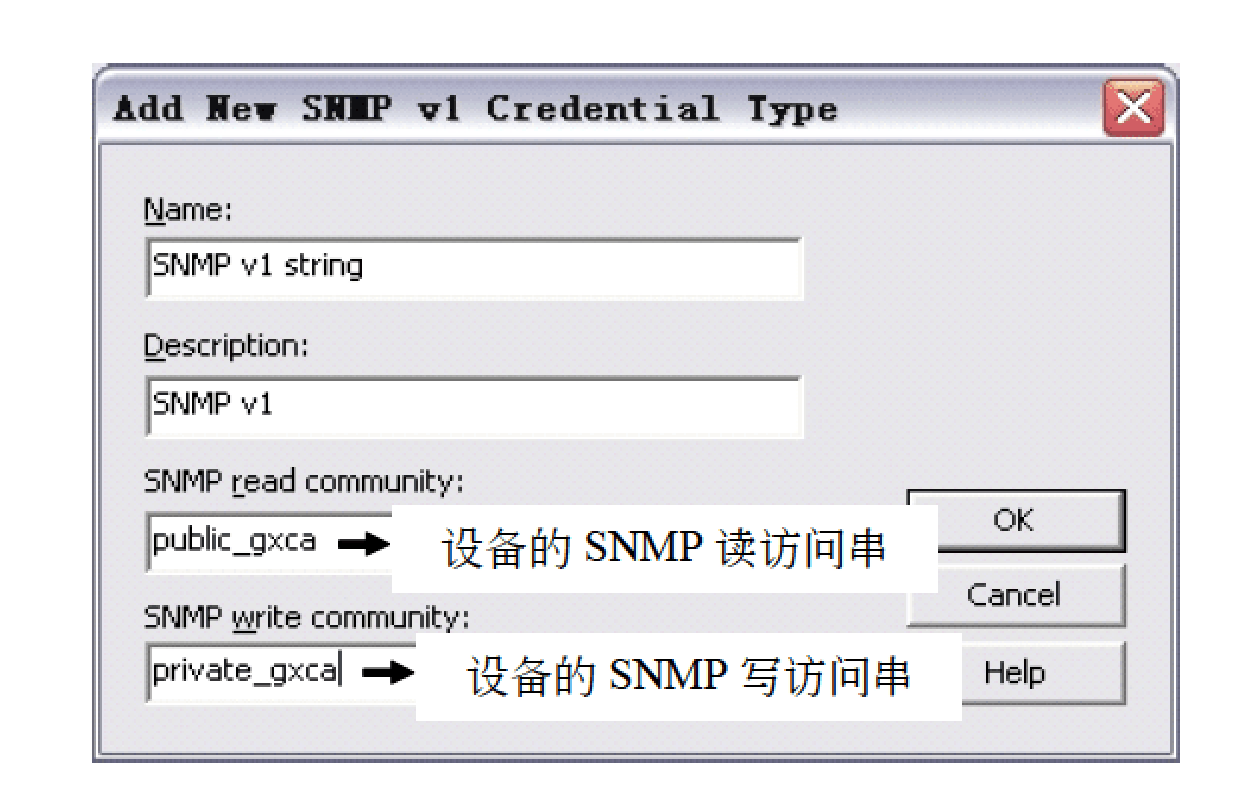


图 6-50　新建 SNMP v1 类型的访问凭证

注意： *在使用凭证的时候，如果需要通过 WMI 方式访问 Windows 主机，那么必须选择 Windows 登录凭证，该方式下无法使用 SNMP 的访问凭证。同样，如果是通过 SNMP 协议访问 Windows 主机，那么必须选择 SNMP 访问凭证。*

6.2.8　Polling 轮询

1．在设备属性中设置轮询 Polling

轮询为 WhatsUp Gold 中的一种主动监测方式，它能够通过多种方式实现，具体依赖于对设备进行的监测内容配置。默认的轮询方式为向设备发送 Ping（ICMP）请求，其周期为 60 秒（可自定义）。主程序通过向被监测的对象发送很小数量级的数据包请求，如果设备状态为正常启用，则将对请求响应，未对请求响应的设备被认为是关闭或停止运行的。

选择属性界面的 Polling 页面，可打开轮询配置界面，如图 6-51 所示。

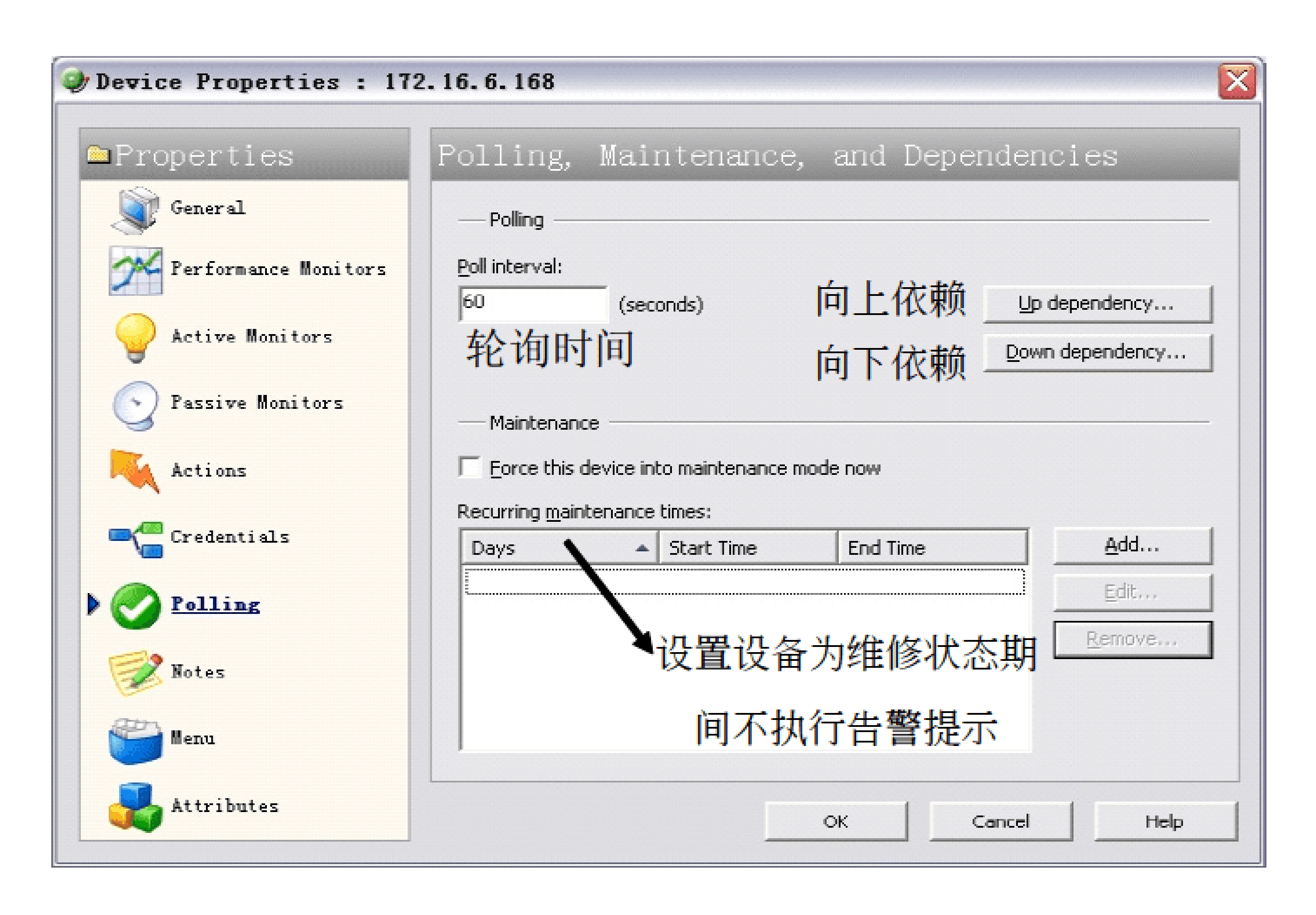


图 6-51　轮询配置界面

在图 6-51 中右下方的 Maintenance 设置界面中，选中 Force this device into maintenance mode now 复选框，可将设备设置为维修状态。该状态下将停止对设备轮询，也不会触发任何报警动作，但该设备仍保留在设备列表中，设备历史数据也被保留在数据库中。

如果需要按时段来设置设备为维修状态，可单击 Add 按钮，打开维修状态的日程安排（如图 6-52 所示），选择周一至周日的一天或多天，选择时段后在指定时间段，该设备将被设置为维修状态。

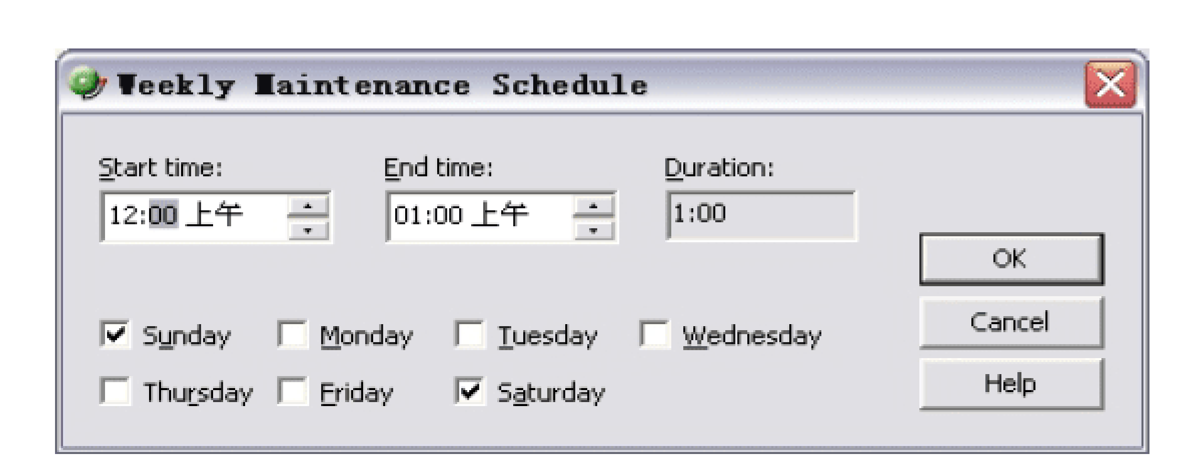


图 6-52　维修状态的日程安排

注意：维修状态的设备在列表中显示为橘黄色的图标。在拓扑视图中显示为。

2. 设置 Polling 依赖关系

通常，WhatsUp Gold 轮询设备列表中所有设备和主动监测项目，除非手动关闭了不需要轮询的对象，例如关闭对整个网络的轮询，或关闭对某一设备、某一监测项目的轮询。轮询的依赖关系能够避免直接关闭对设备的轮询进程，而是依赖于其他设备的运行状态。

在 Polling 设置界面中可更改设备之间的依赖关系。设备间的依赖关系分为两种，向上依赖和向下依赖：

- 向上依赖（Up Dependency）：可以理解为一个设备是依赖于另一设备之后的，只有在其之前的设备状态是正常运行的，才会展开对该设备的轮询。
- 向下依赖（Down Dependency）：可以理解为一个设备是处于另一设备之前的，存

在该依赖关系的设备，只有当它之后的设备有进一步状态改变（断开或关闭等），才会展开对该设备的轮询。

例如，将某设备置于路由器之后，并将设备定义为向上依赖于路由器的 Ping 主动监测，则只有对路由器的 Ping 操作是成功的，才会对该设备采取轮询。如果对路由器 Ping 操作失败，那么置于路由器之后的设备将被设置为状态不可知，而不再去轮询该设备。如果没有该依赖机制，位于路由器后面的设备由于路由器的关闭，状态变为 Down 并会持续不断地触发报警提示信息。由于该依赖机制，只有路由器会触发报警提示。

在 Polling 界面中，通过单击 Up Dependency 或 Down Dependency 按钮，可为设备添加依赖关系。此处先选择配置向上依赖关系，其图标显示为向上的绿色箭头，如图 6-53 所示。

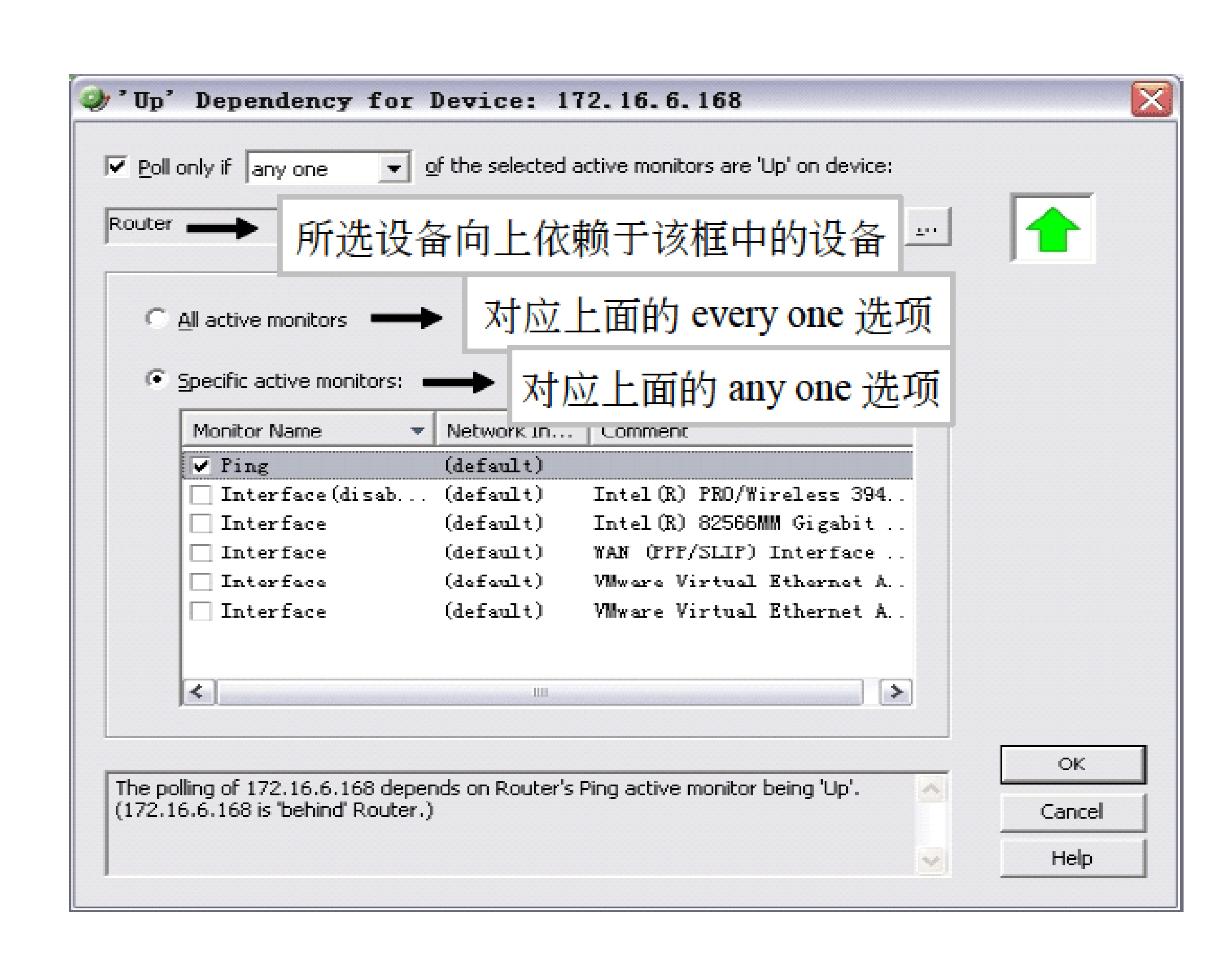


图 6-53　Polling 中设置向上依赖关系

图 6-53 中，首先单击 Router 文本框右侧的浏览按钮，为当前 PC 设备选择其向上依赖的对象。此处我们选择一台路由器，即该设备向上依赖于路由器的状态。然后选择 Poll only if 复选框，并选择下拉列表选项。选项介绍如下：

- Any one：列出的路由器的主动监测项目中，有其中任意一项状态为 Up，就会启动对 PC 设备的轮询。例如，只要可以在 Specific active monitors 选择任一项或多项，当选择项目状态为 Up 时，对 PC 设备启动轮询。
- Every one：列出的路由器主动监测项目中，每一项监测项目状态均为 UP，才会启动对该 PC 设备的轮询。即在 Specific active monitors 中列出的监测项，当所有监测项目状态为 UP 时，才对该设备启动轮询操作。

向下依赖界面的配置类似于向上依赖的配置方法，如图 6-54 所示。

3. 在拓扑图模式中设置依赖关系

在控制台中，选择 View | Map View 命令，进入到拓扑图窗口中，如图 6-55 所示。

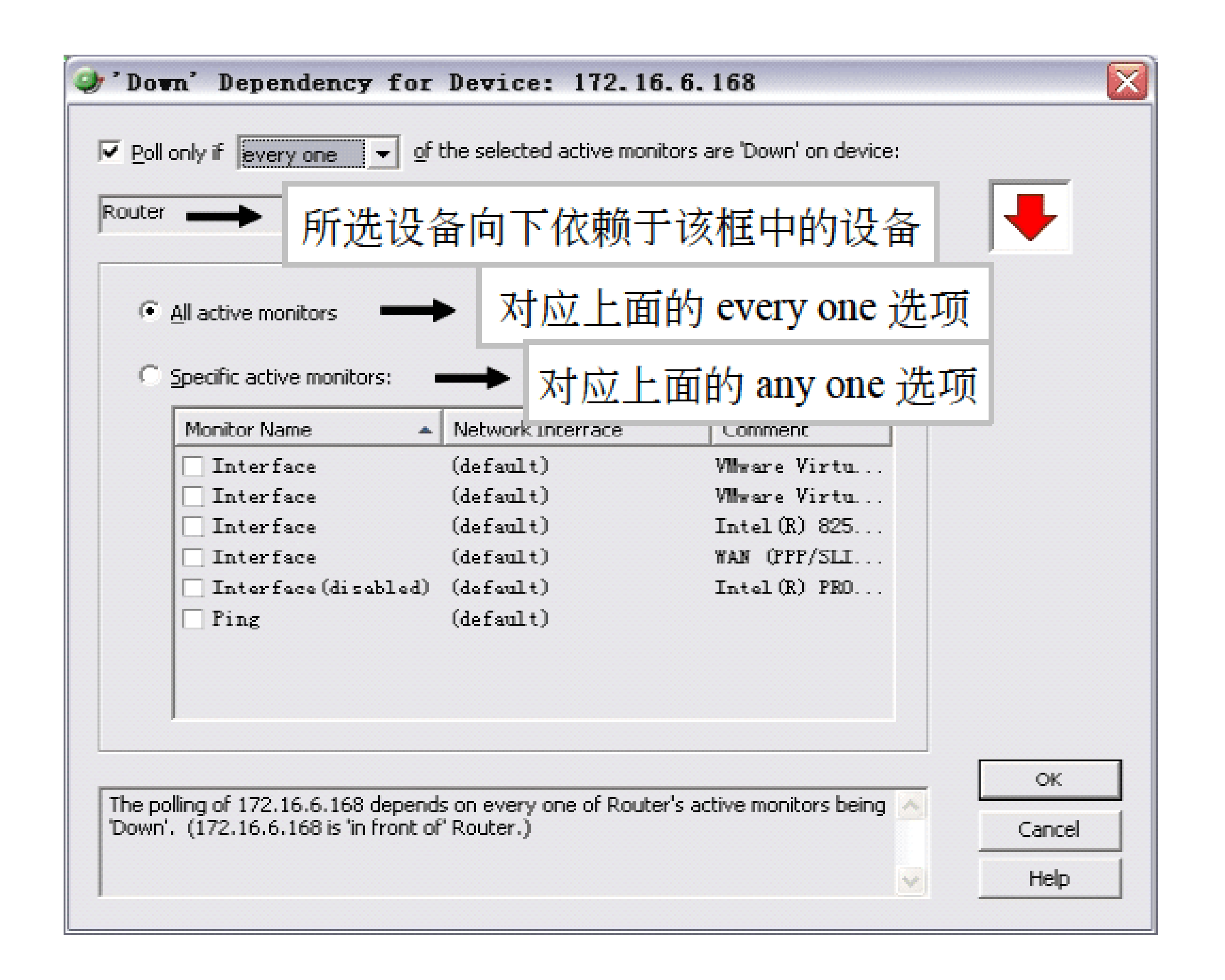


图 6-54 Polling 中设置向下依赖关系

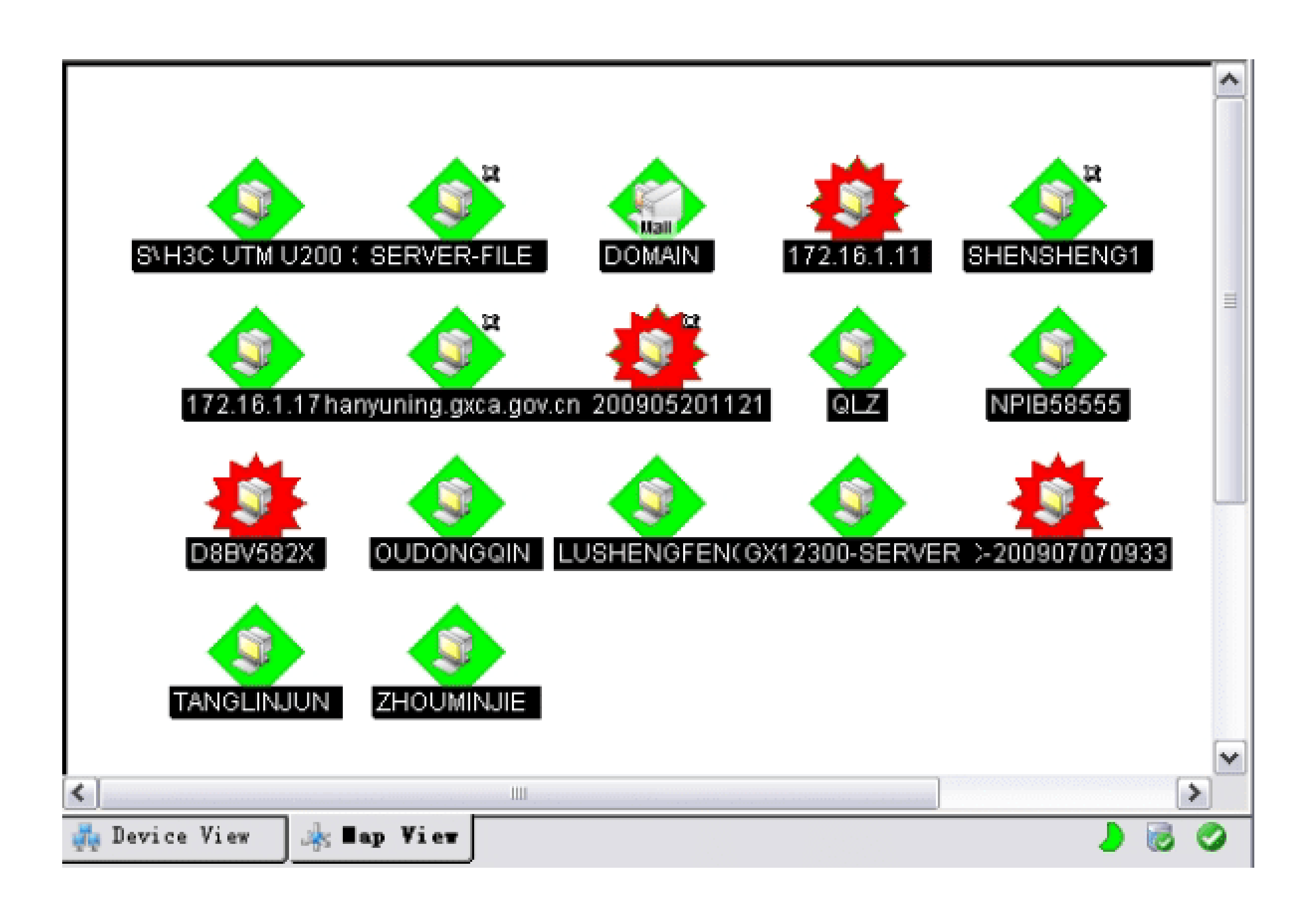


图 6-55 Map 视图

右击某设备，打开右键菜单，选择 Set Dependencies 命令，为设备添加依赖关系和清除。此处，选择 Up Dependency 或 Down Dependency，鼠标将变为带箭头指示的图标，如图 6-56 所示。



图 6-56 Set Dependencies

鼠标变为带箭头后选择与该设备建立依赖关系的另一设备，在弹出的对话框中后选择设备的监测项目已经被加入到界面中，选择需要建立依赖关系的主动监测项目即可。

建立依赖关系之后，可以在 Map 视图中查看依赖关系。在 Map 视图中打开右键菜单，选择 Display | Polling Dependency Arrows，则会显示设备间的依赖关系，如图 6-57 所示。

实例：在图 6-57 中，主机设备向上依赖于路由器，路由器向下依赖于集线器。如果路由器的主动监测项目变为非活跃状态，路由器向下依赖于集线器，那么集线器将被轮询。在路由器之后的主机则不轮询。当路由器的主动监测项目为激活状态，那么位于该路由器之后的主机设备被轮询，而集线器不轮询。

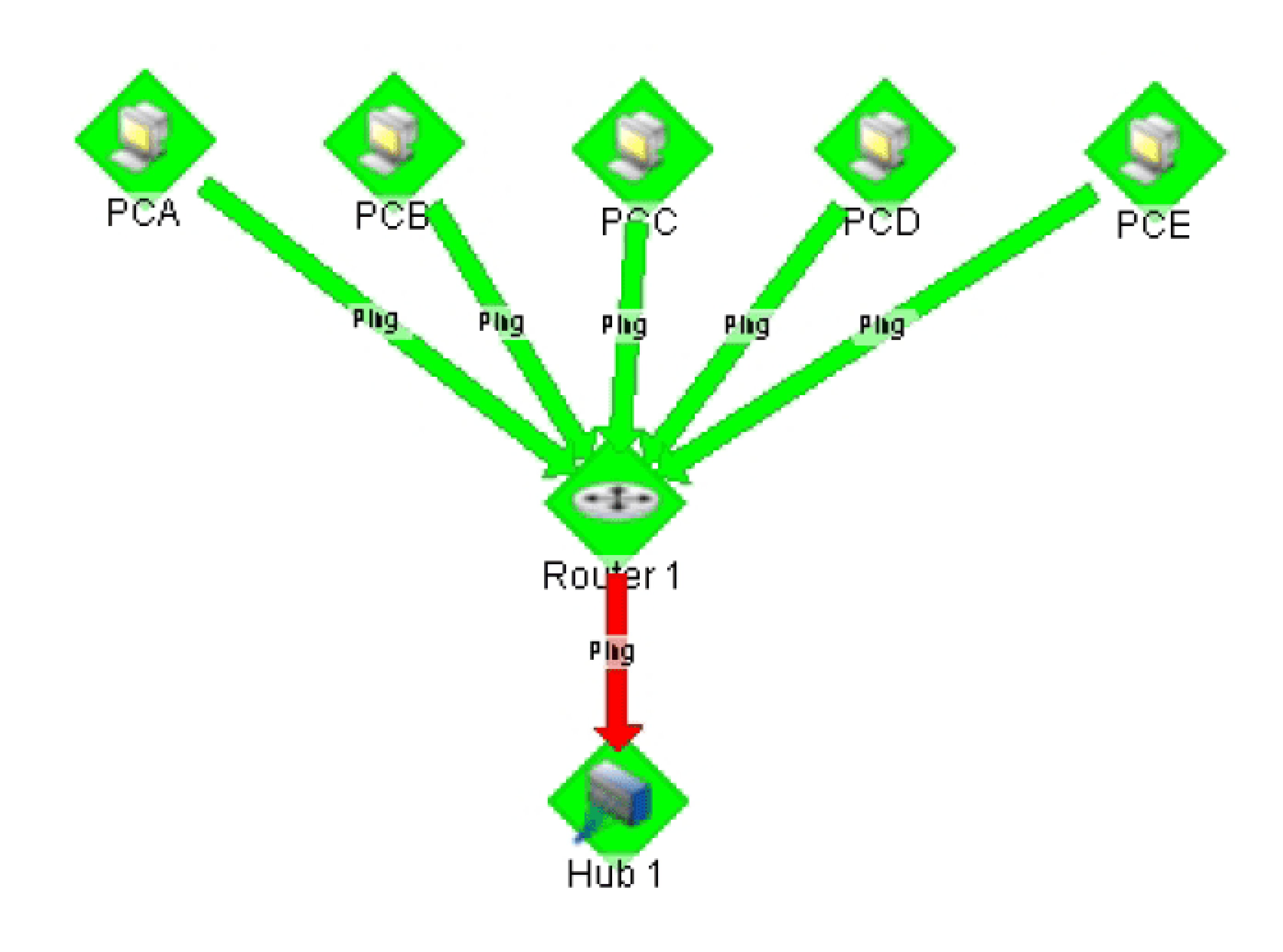


图 6-57　查看设备依赖关系

注意：不能跨越设备组对设备建立依赖关系。尽管如此，可以通过在一个组中添加另一组中某设备的快捷图标，然后通过该快捷图标建立依赖关系。

4. 启动和停止设备轮询

通过启动和停止 WhatsUp Gold 轮询引擎，来控制对设备是否进行轮询。在主界面菜单中选择 Configure | Program Options 命令，并在界面中选择 General 页面，如图 6-58 所示。

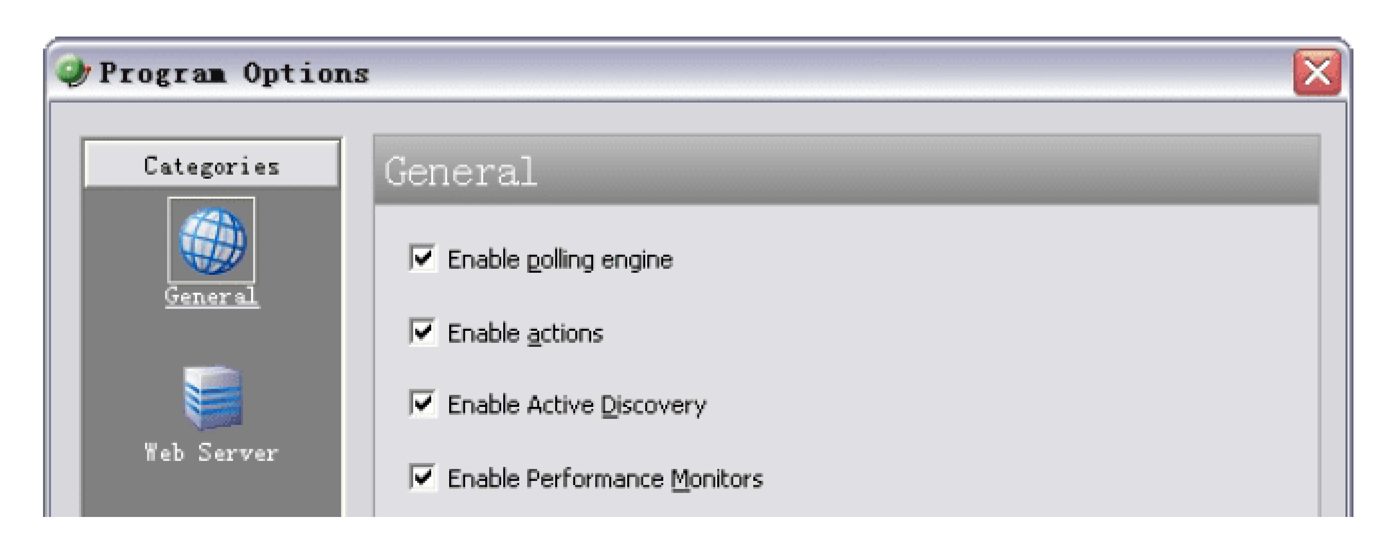


图 6-58　启动和停止轮询

- 选择 Enable polling engine 则允许轮询设备，否则关闭轮询。
- 选择 Enable actions 允许当设备发生状态改变时，触发提示动作的执行。
- 选择 Enable Active Discovery 允许通过 SNMP 等方式自动发现设备。
- 选择 Enable Performance Monitors 允许开启性能监测项目。

5. 启动和停止监测项目轮询

轮询机制除了针对整个设备设置是否启动，还能对设备的单个监测项目做配置。选择某设备，打开属性界面，选择 Active Monitor 页面，并选择某项监测项目，然后单击 Edit 按钮，打开编辑窗口，如图 6-59 所示。

选择 Enable polling for this Active Monitor 复选框，则允许轮询该监测项目，否则停止轮询。



图 6-59 对个别监测项目配置允许 Polling

6.2.9 Notes 备注事项

在 Notes 选项中，第一行信息为添加该设备到数据库中的日期和时间。可以在空白文本框中输入任何备注信息，例如设备的历史记录、物理位置等信息，如图 6-60 所示。

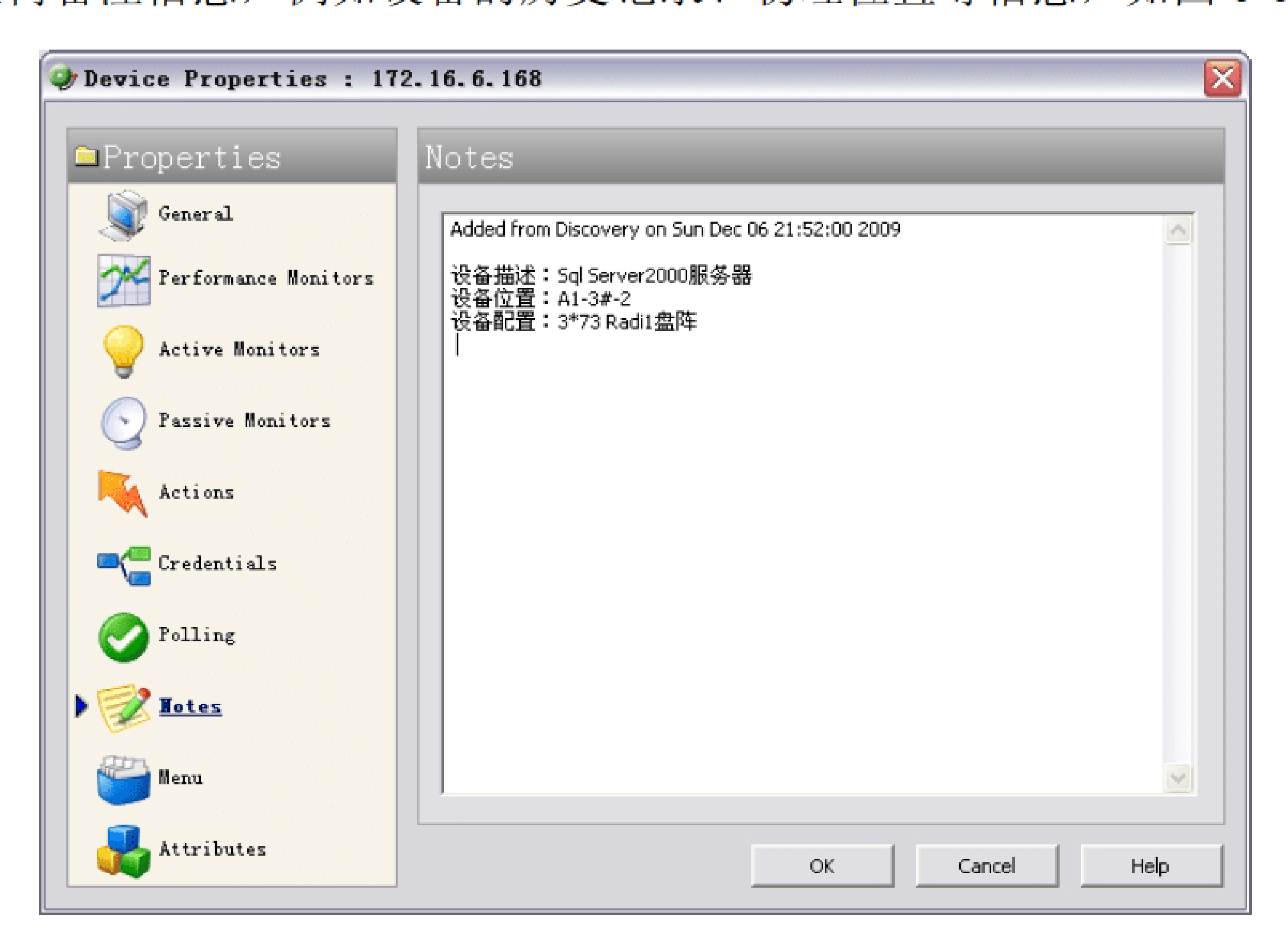


图 6-60 为设备添加备注信息

6.2.10 Menu 右键菜单命令

在 Menu 选项中，可为所选设备配置其右键菜单命令，可为右键菜单中添加、修改或删除命令。例如，添加直接调用外部程序、执行 CMD 命令或批处理命令等项目。

在 Menu 列表中，WhatsUp Gold 默认提供了 4 个快捷工具，分别是通过 IE 浏览器访问该设备地址、Telnet 设备、执行 Ping 设备以及 Traceroute 设备。例如，选择菜单命令 Ping

即完成对设备的 Ping 操作等，省略了输入 Ping 命令的步骤，如图 6-61 所示。

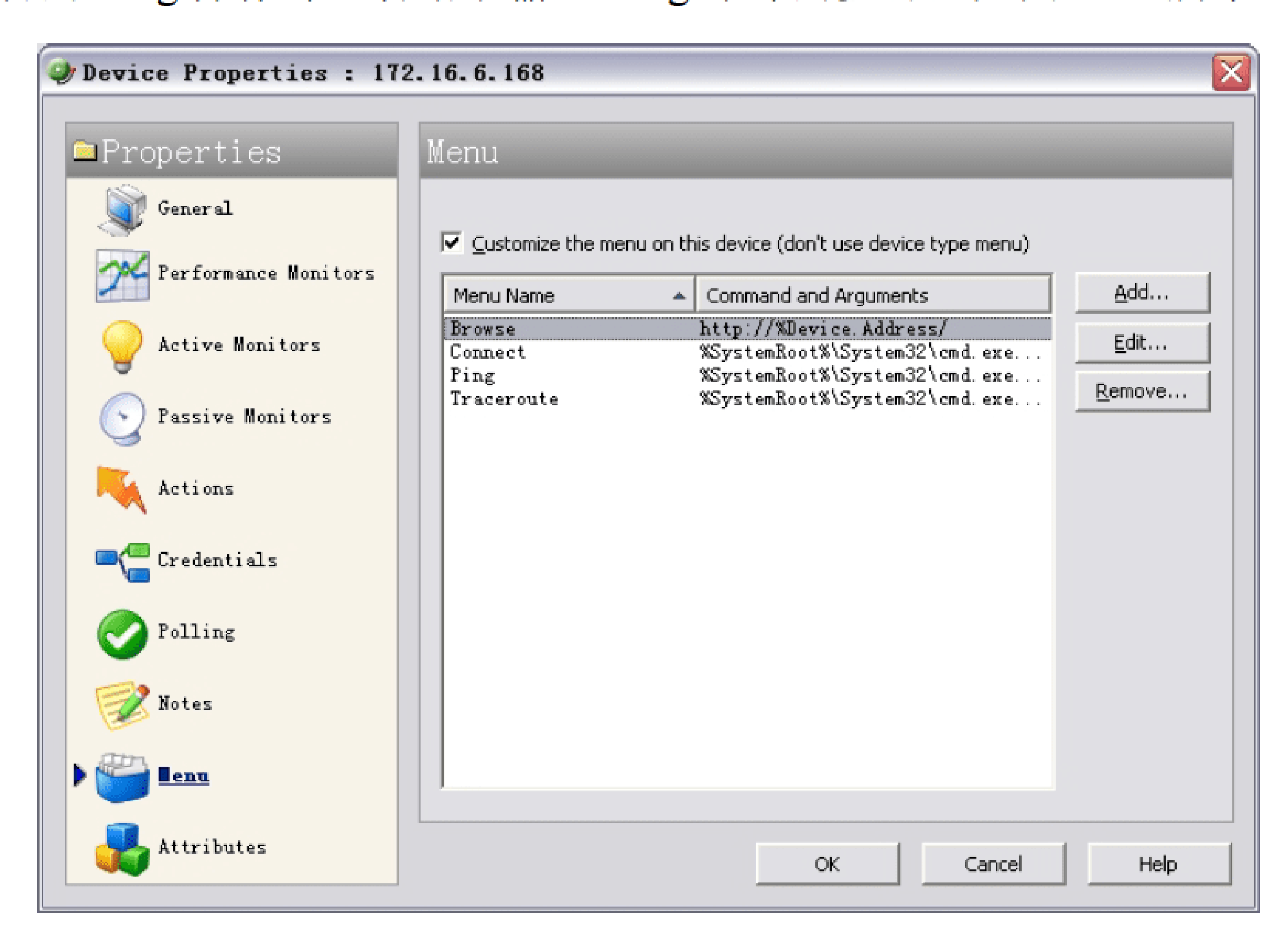


图 6-61　Menu 选项配置

要为该设备增加快捷命令，首先需要选中 Customize the menu on this device 复选框，允许客户自定义右键菜单命令，然后单击 Add 按钮，打开新增对话框。

示例 1：为该设备新增查看端口的快捷命令 Netstat，如图 6-62 所示。

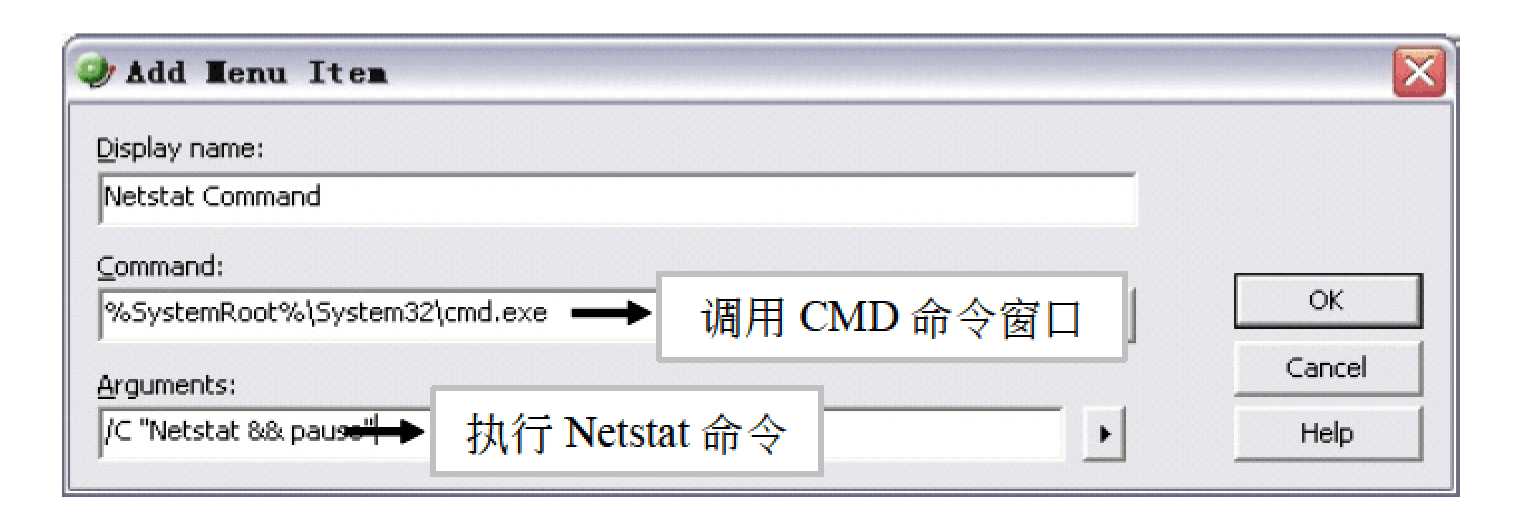


图 6-62　添加右键菜单命令

在 Display name 中输入该新增右键菜单命令的名称；在 Command 下拉列表框中选择调用 CMD 命令窗口；在 Arguments 文本框中输入要执行的命令为 Netstat，确认即完成添加。

示例 2：为该设备新增调用 SecureCRT 的外部程序，并运行 Top 命令查看 CPU 状态，只需选择外部程序的路径即可，如图 6-63 所示。

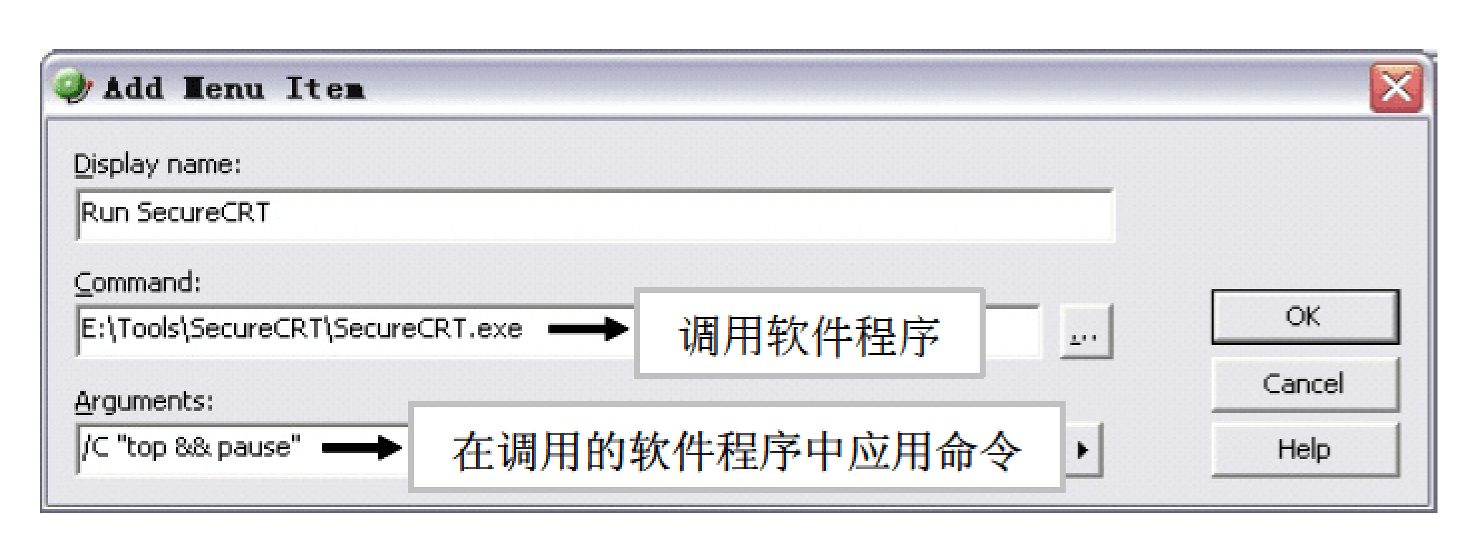


图 6-63　调用 SecureCRT 程序

在为该设备增加如上两项右键菜单命令后，在该设备上打开右键快捷菜单，将看到添加的两个命令，如图 6-64 所示。

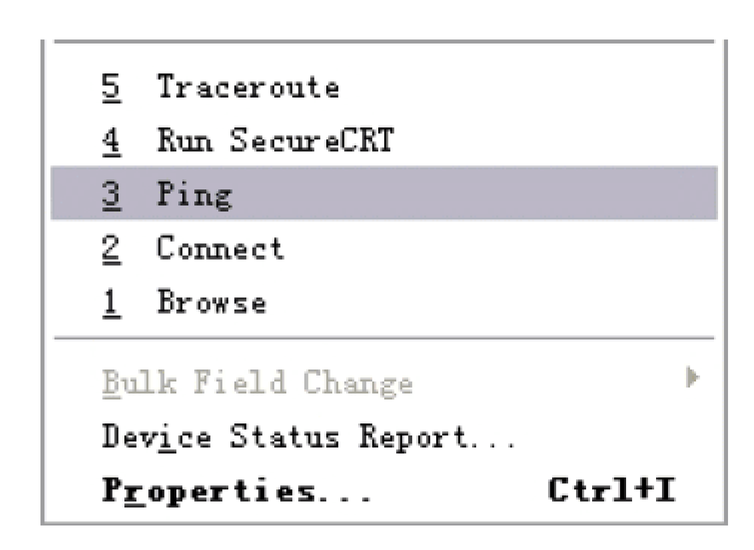


图 6-64 查看右键菜单

6.2.11 Attribute 增加附加属性

在 Attribute 页面中可为所选设备增加附加属性。在界面中默认包含了 3 个附加属性，包括联系人、描述信息和物理位置信息。可以通过单击 Edit 按钮完善信息，单击 Add 按钮添加新的附加信息，如图 6-65 所示。

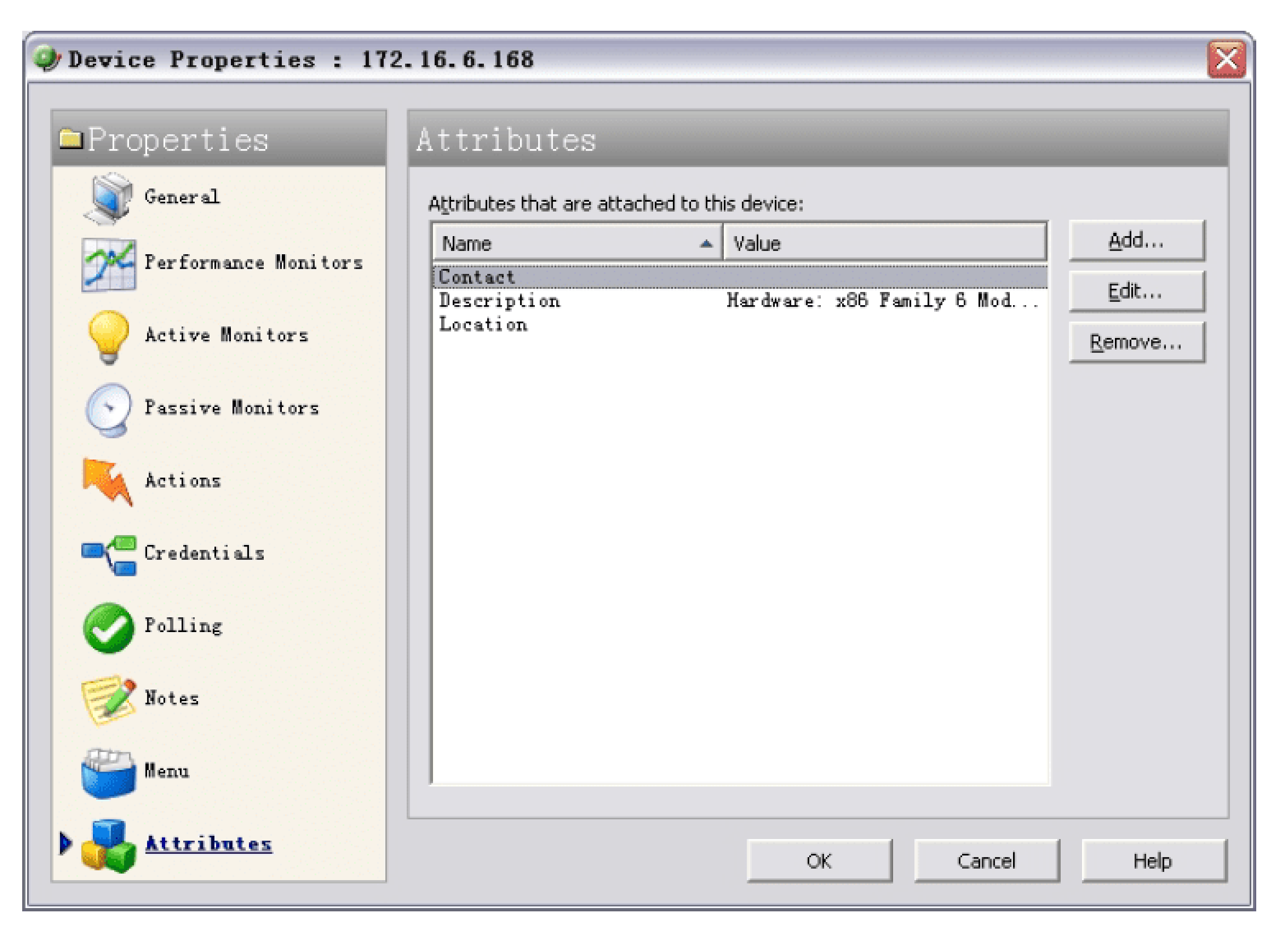


图 6-65 设备的 Attribute 属性

6.2.12 界面快捷菜单及附加工具

主界面的快捷菜单中的命令和程序自带的一些附加工具，能够帮助网络管理员更直观和快捷地了解网络设备的一些特定信息。在设备列表或 Map 视图中，右击打开快捷菜单，如图 6-66 所示。

在右键菜单中可新建设备、设备组和动态设备组，查看设备报表和组报表信息，以及复制、删除和重命名设备等。这些命令均为常用命令，以下分别介绍快捷菜单命令的功能。

1. SNMP View 工具

SNMP View 辅助工具采用 SNMP 协议采集设备信息。首先选择某交换机设备，在该设备上右击，选择 SNMP View 菜单命令，在弹出的 SNMP 窗口中列出了交换各个端口，并以颜色显示端口状态。绿色表示该端口状态为 UP，红色表示该端口状态为 Down，灰色表示端口已经启用但无数据流，如图 6-67 所示。

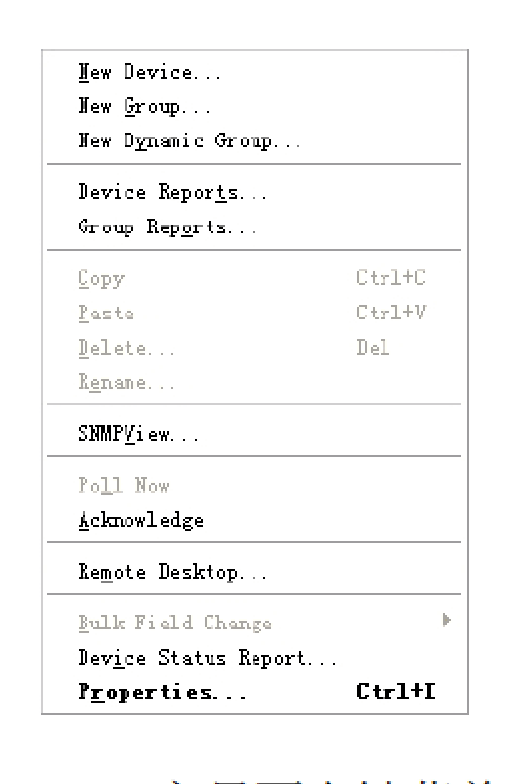


图 6-66　主界面右键菜单

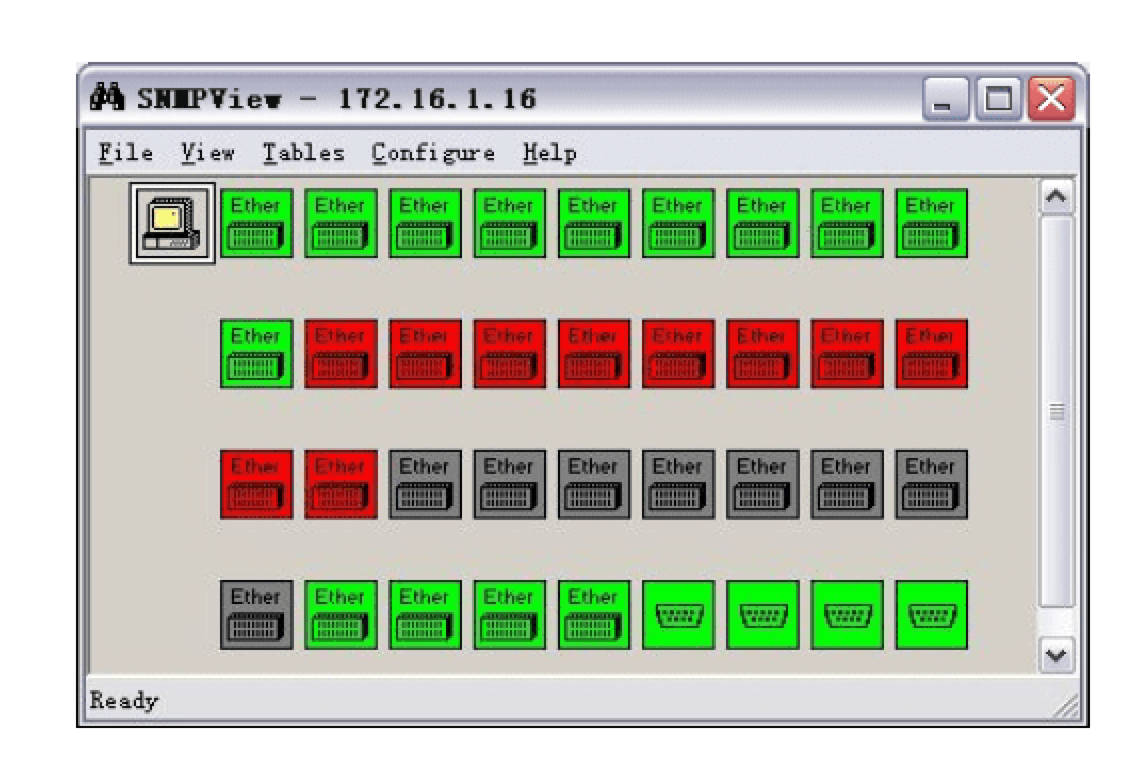
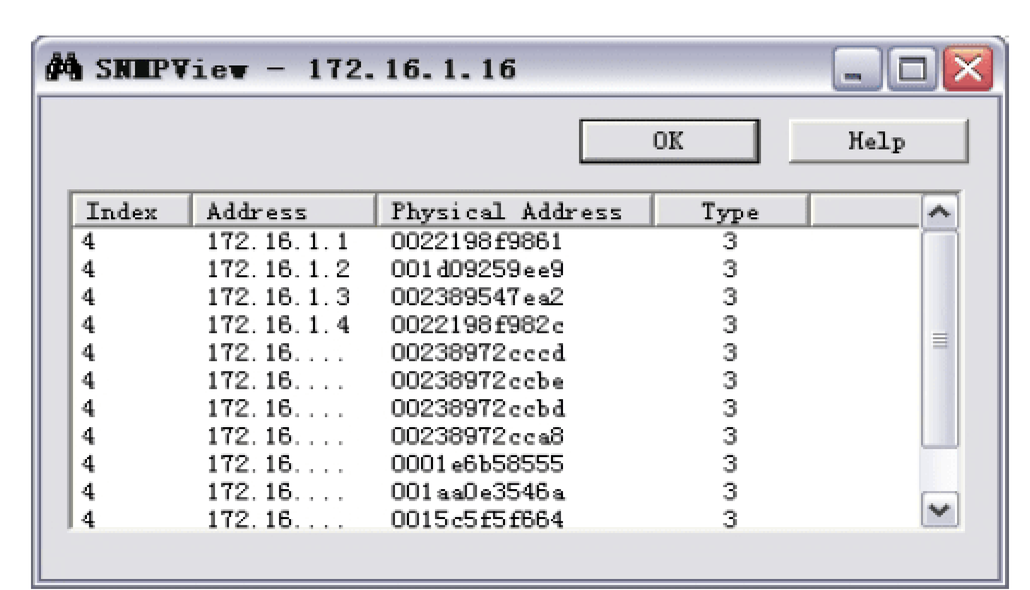


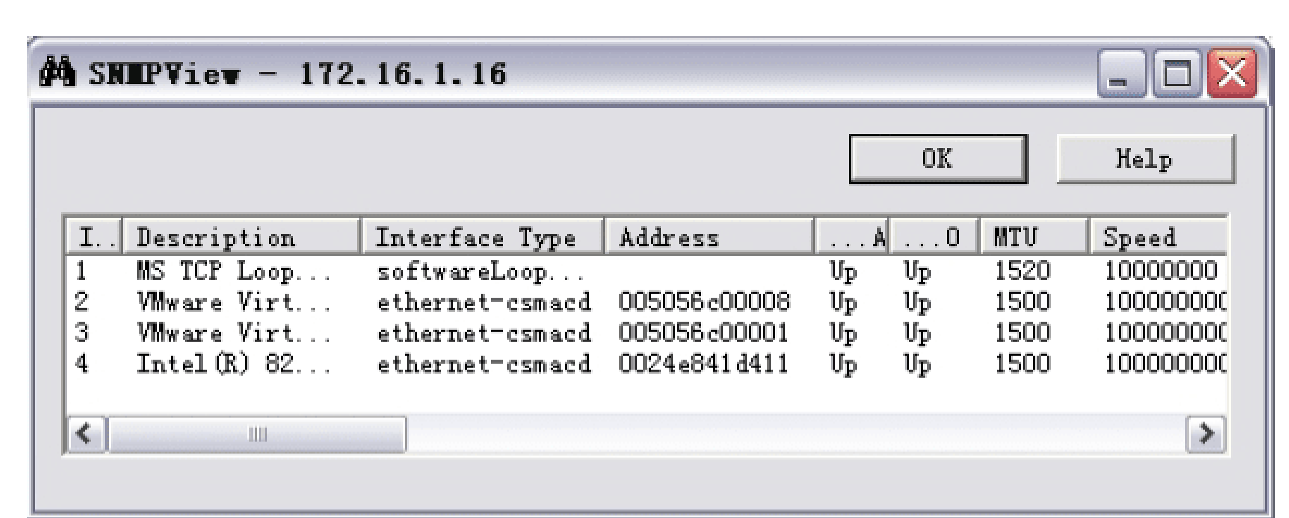
图 6-67　SNMP View 查看设备端口

在 SNMP View 界面中选择主菜单 Tables | ARP Table 命令，可打开 ARP 表（Address Resolution Protocol，地址解析协议），其中罗列出了 IP 与网卡 MAC 地址的对照表，如图 6-68 所示。

选择主菜单 Tables | Address Table 命令，可查看设备的 IP 地址表；选择 Tables | Interface Table 命令，可查看设备的各个端口列表信息，如图 6-69 所示。



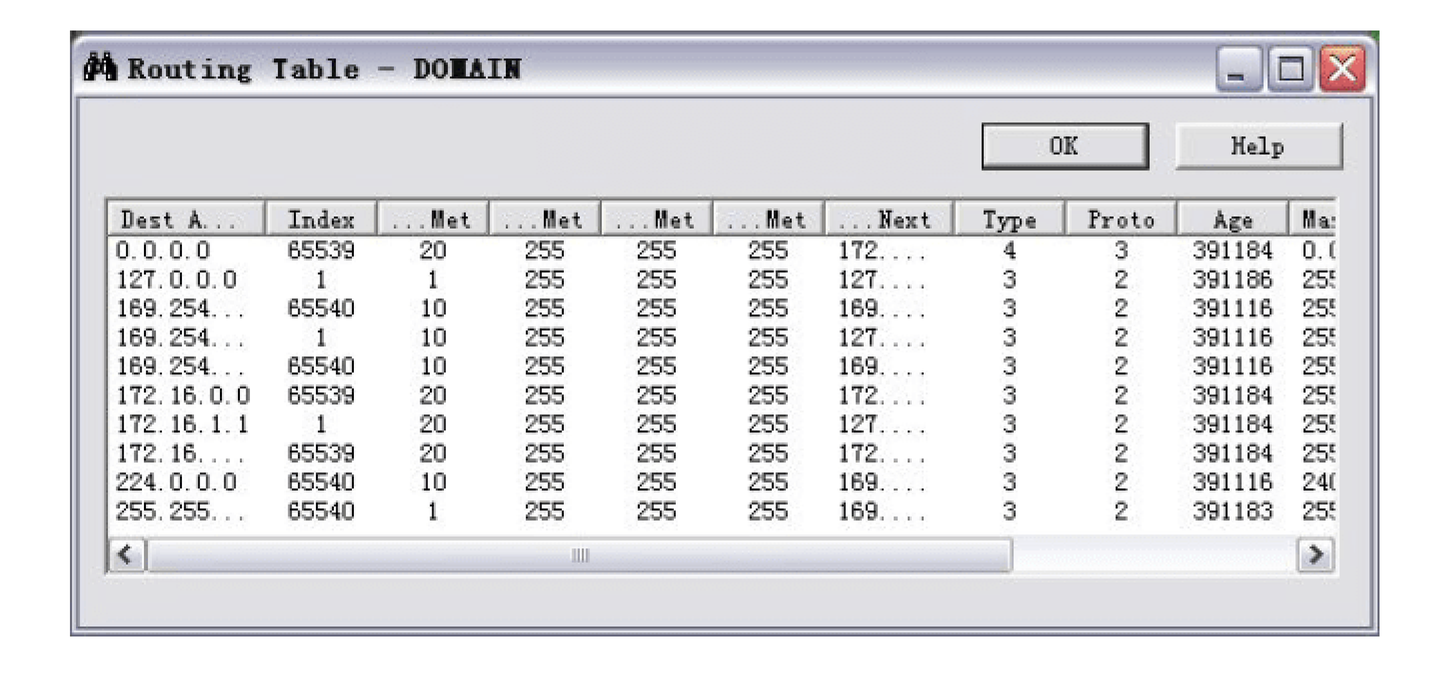
Index	Address	Physical Address	Type
4	172.16.1.1	0022198f9861	3
4	172.16.1.2	001d09259ee9	3
4	172.16.1.3	002389547ea2	3
4	172.16.1.4	0022198f982c	3
4	172.16....	00238972cccd	3
4	172.16....	00238972ccbe	3
4	172.16....	00238972ccbd	3
4	172.16....	00238972cca8	3
4	172.16....	0001e6b58555	3
4	172.16....	001aa0e3546a	3
4	172.16....	0015c5f5f664	3



I...	Description	Interface Type	Address	...A	...O	MTU	Speed
1	MS TCP Loop...	softwareLoop...		Up	Up	1520	10000000
2	VMware Virt...	ethernet-csmacd	005056c00008	Up	Up	1500	10000000(
3	VMware Virt...	ethernet-csmacd	005056c00001	Up	Up	1500	10000000(
4	Intel(R) 82...	ethernet-csmacd	0024e841d411	Up	Up	1500	10000000(

图 6-68　ARP 表　　　　图 6-69　查看设备端口

选择主菜单 Tables | Route Table 命令，可查看设备的路由表信息，其中包含了设备 IP 地址的路由指向、其下一跳地址及跳数等信息，如图 6-70 所示。



Dest A...	Index	...Met	...Met	...Met	...Met	...Next	Type	Proto	Age	Ma
0.0.0.0	65539	20	255	255	255	172....	4	3	391184	0.(
127.0.0.0	1	1	255	255	255	127....	3	2	391186	25!
169.254...	65540	10	255	255	255	169....	3	2	391116	25!
169.254...	1	10	255	255	255	127....	3	2	391116	25!
169.254...	65540	10	255	255	255	169....	3	2	391116	25!
172.16.0.0	65539	20	255	255	255	172....	3	2	391184	25!
172.16.1.1	1	20	255	255	255	127....	3	2	391184	25!
172.16....	65539	20	255	255	255	172....	3	2	391184	25!
224.0.0.0	65540	10	255	255	255	169....	3	2	391116	24(
255.255...	65540	1	255	255	255	169....	3	2	391183	25!

图 6-70　查看设备的路由表信息

2. 批量设置功能 Bulk Field Change

批量设置功能，允许程序对设备的共有属性做批量设置，该设置能极大地减少工作量。

首先按住 Shift 键选择多个设备，然后在这些设备上打开右键菜单，并选择 Bulk Field Change 命令，批量设置访问凭证、轮询时间、设备类型、轮询时间周期、备注及依赖关系等。

例如，可为多个设备设置访问的登录凭证 public，包括 Windows 登录和 SNMP 访问凭证。可设置为共同社区字符串 public 或者不改变设备原来的选项 No change，如图 6-71 所示。

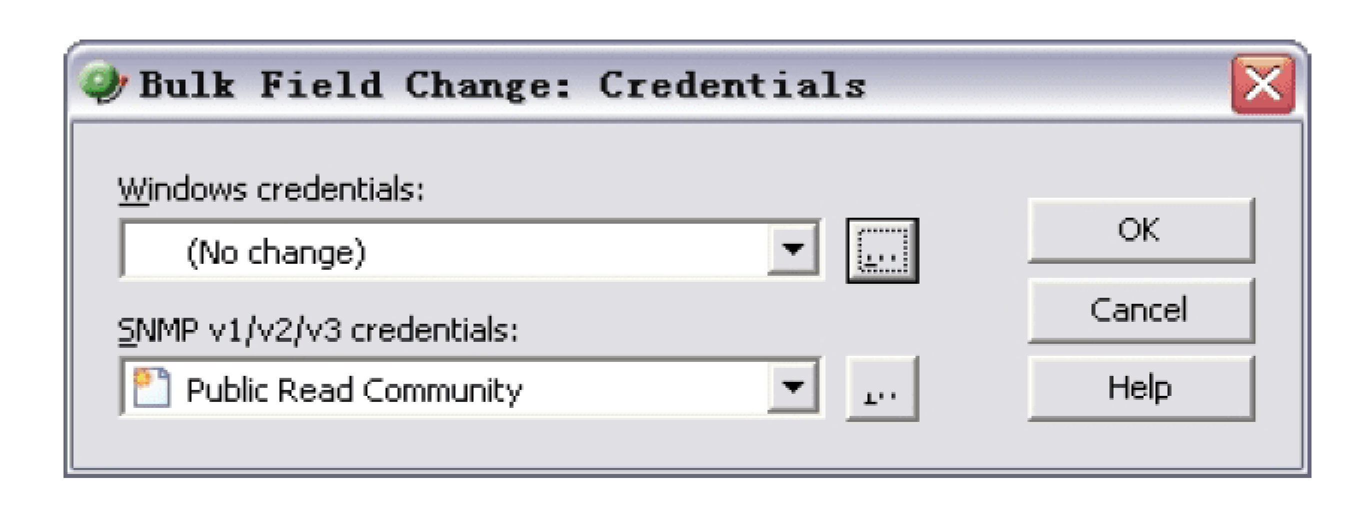


图 6-71　批量设置设备的访问凭证

3. 确认功能 Acknowledgements

当设备状态发生改变时，无论已经执行了何种报警提示动作，在设备列表和 Map View 视图中，仍将对设备图标做出标识提醒你的设备状态的改变。设备列表中将设备名显示为粗体，在 Map View 视图中，设备名称将显示为黑色的背景颜色如图 6-72 所示。

当在该设备上打开快捷菜单并选择 Acknowledgements 命令时，表示已经明确了该设备状态的变化。可以取消提示，图标将恢复正常状态显示。

图 6-72　设备名称显示为黑色的背景

4. 附加工具 Net Tools

选择主界面菜单 Tools | Net Tools 命令，打开附加程序窗口，该工具中包含了常用网络测试小工具，例如集成了 Ping 命令、采集 SNMP 的 MIB 对象参数值、按网段扫描设备等常用工具，能帮助网管员进行简单的测试等操作，如图 6-73 所示。

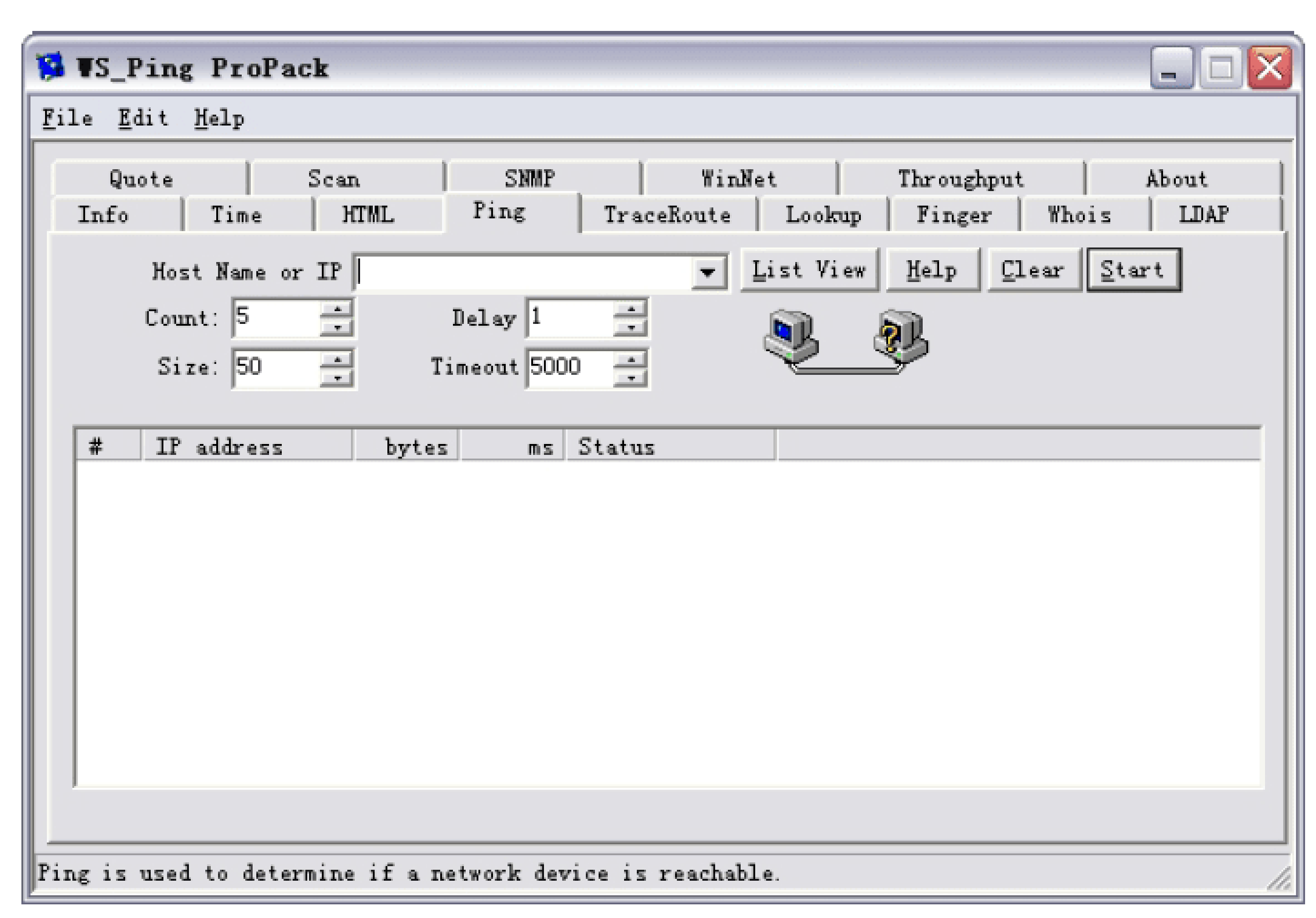


图 6-73　Net Tools

6.3 报警提示动作及动作策略配置

6.3.1 报警提示功能介绍

WhatsUp Gold 通过轮询的信息反馈或接收到的 Trap 消息监测网络设备。一旦网络中发生任何状态的变化，都能通过设置执行某些动作作为报警或提醒。例如，在 Ping 设备无应答时，可配置执行声音提醒、邮件提醒或调用外部程序等提示动作，这些提示能够帮助管理员迅速发现和解决问题。

在 WhatsUp Gold 中，可以对某一设备和监测对象逐个添加要执行的提示动作。为了避免重复为每个设备添加多个报警动作，可以将几种提示动作组合在一起配置成一个动作策略（Action Policy），该策略是一组动作的组合。配置完成后，将保存于动作策略库中，供不断新增的设备和监测对象直接调用。

注意：当某设备要求增加特别的提示动作或不需要执行某动作策略时，可根据需要单独为其配置所需要的报警执行动作。

6.3.2 配置单一提示动作及实例

在 Action Library（提示动作库）中列出了所有系统和自定义配置的提示动作。这些动作能够添加到网络中任何设备或监测项目上，或包含于某个 Action Policy（动作策略）中。

1. 查看提示动作的配置

选择主界面菜单中的 Configure | Action Library 命令，打开动作库配置界面，该界面可对现有动作进行修改、删除及添加新的提示动作。如需查看某提示动作的具体配置信息，可通过双击该动作选项进行查看。此处，双击系统自带的 Sound-Down5 选项，当设备或服务停止响应超过 5 分钟时，WhatsUp Gold 将发出声音提醒，如图 6-74 所示。



图 6-74　查看 Down5 分钟时的声音提醒

2. 新建报警提示动作

在 Action Library 界面中，单击 New 按钮弹出新建对话框，在动作类型列表框中列出了可添加的动作类型，如图 6-75 所示。每次添加新的提醒动作，都会被加入到 Action Library 中，供再次使用时直接调用。在该界面中，还可以修改、复制和删除动作。

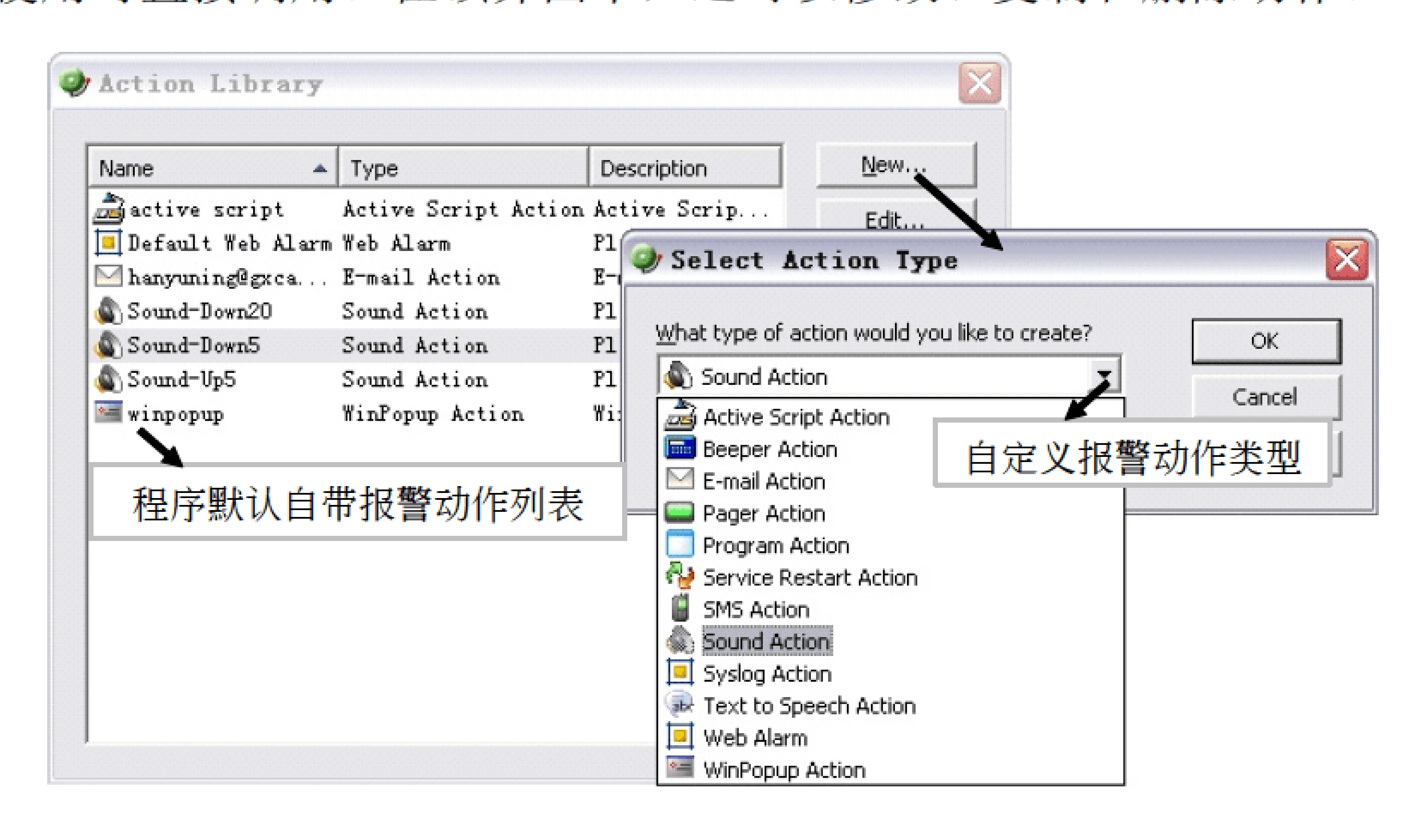


图 6-75　动作库配置及新建动作

🔔注意：在删除某一执行动作，如果该动作同时属于某个策略时，那么该动作也从策略组中被删除。

添加某报警动作后，可在动作库界面中单击 Test 按钮，对该动作进行测试，如图 6-76 所示。

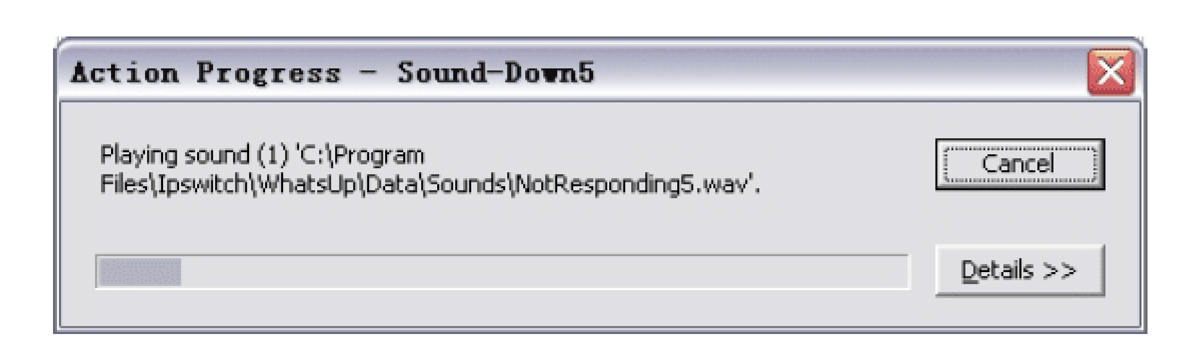


图 6-76　测试执行动作

在新增动作下拉列表中，WhatsUp Gold 提供以下几种动作类型。

- ❑ Active Script Action：执行脚本文件。可编写 VBScript 或 JScript 脚本执行对设备执行核查。如果检查某对象返回错误代码，那么认为该对象是关闭或无法连接的。
- ❑ Beeper Action：执行声音提醒。通过 Modem 连接电话机，并在 Action 中设置呼叫的号码，触发电话机发出提示音。
- ❑ Email Action：通过邮件服务器的 SMTP 服务发送 E-mail 邮件提示。
- ❑ Pager Action：寻呼机提醒。通过设置 Modem 信息、呼叫的寻呼机号码、密码、标识号及协议等，发送报警消息至寻呼机。
- ❑ Program Action：调用外部程序。通过启动一个可执行的外部程序执行某动作。
- ❑ Service Restart Action：重启服务。关闭或者重启 Windows 系统制定服务。

- SMS Action：发送短消息。通过发送 SMS（Short Message Service 短信息）到手机。
- Sound Alarm：声音提醒。播放指定声音文件作为提醒，在 WhatsUp Gold 中可在 6 个时间点设置发出声音提醒，包括设备停止响应时、停止响应 2 分钟、停止响应 5 分钟、停止响应 20 分钟、恢复正常响应及恢复正常响应 5 分钟。
- Syslog Action：发送系统日志信息。发送日志记录到制定日志服务器（需要在接收日志的服务器上安装日志接收程序，例如较流行的日志分析软件 Kiwi Syslog Daemon）。
- Text to Speech Action：朗读信息。通过声卡将文字提示信息朗读出。
- Web Alarm：网页报警。在 WhatsUp 网页模式下，播放某一声音文件作为提示。
- WinPopup Action：弹出提示框。在 Windows NT 系统中，弹出信息提示框。

注意：由于触发电话机、寻呼机及发送短信息等方式需要配置相应的硬件设施，在此不做介绍，本节通过实例介绍如何添加告警（提示）动作。

实例 1：添加 Email Action

选择 Configure | Action Library 命令，在弹出的对话框中单击 New 按钮，并选择新建动作类型为 E-mail Action，即建立发送 Email 信息的报警动作。

然后，进入下一步配置 E-mail Action。输入自定义名称为 E-mail_Action，并加入描述信息。在 SMTP server 文本框中输入邮件服务器 IP 地址，该报警动作将用到邮件服务器的 SMTP 功能，发送端口使用默认端口 25。在 Mail to 文本中输入接收邮件的邮箱，如果有多个接收邮箱地址，则使用逗号隔开，如图 6-77 所示。

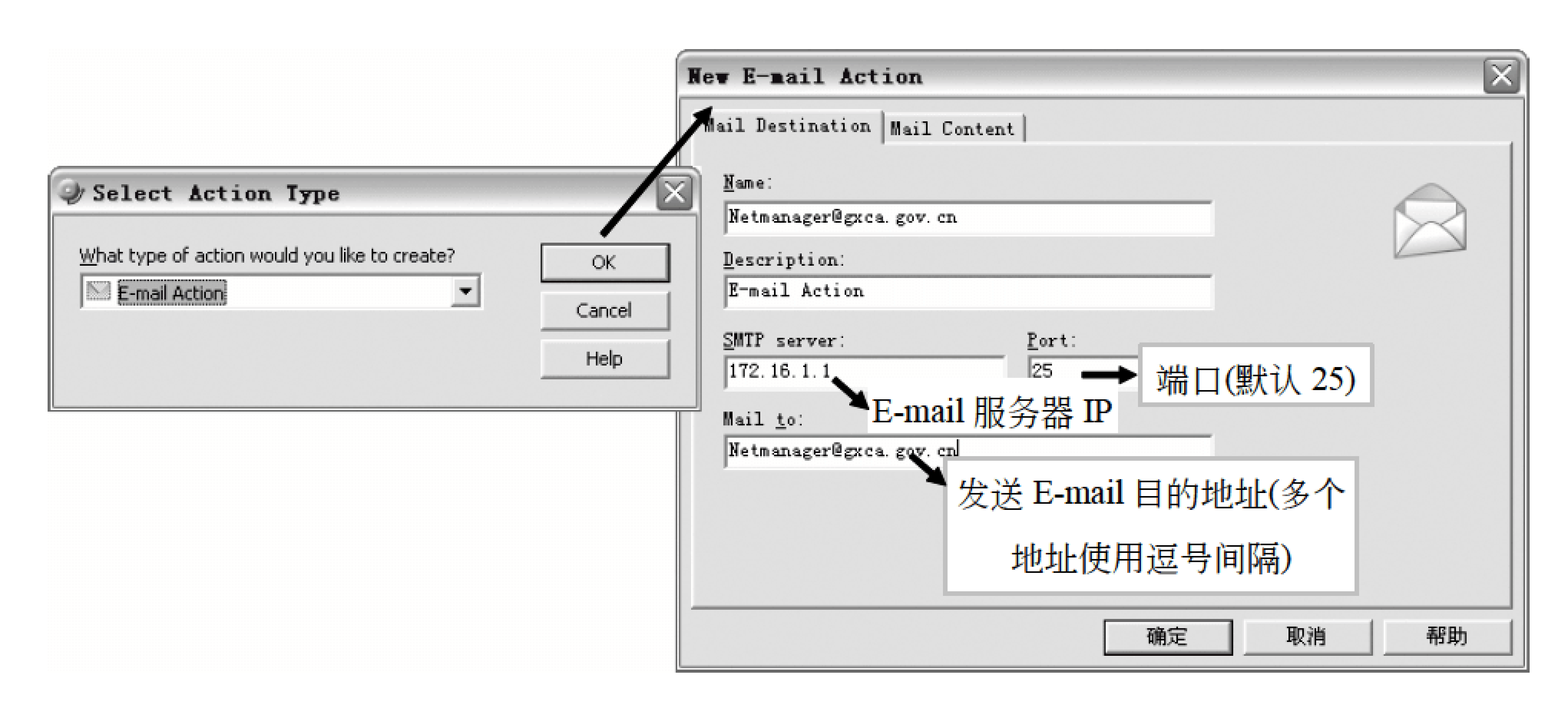


图 6-77 添加 E-mail Action

在 Mail Content 选项页中列出了邮件包含内容，其中包括触发提示动作的设备 IP、状态变化情况、备注信息等。使用默认内容就能够获取足够的信息。

配置结束后在 Action Library 列表中能够看到刚才添加的 E-mail_action，如图 6-78 所示。该动作能够被添加到任何设备或监测服务中。

注意：此处添加的报警提示动作已经保存至动作库中，在为设备或监测项目添加提示动作时，已经可以选择新建的 E-mail 动作。

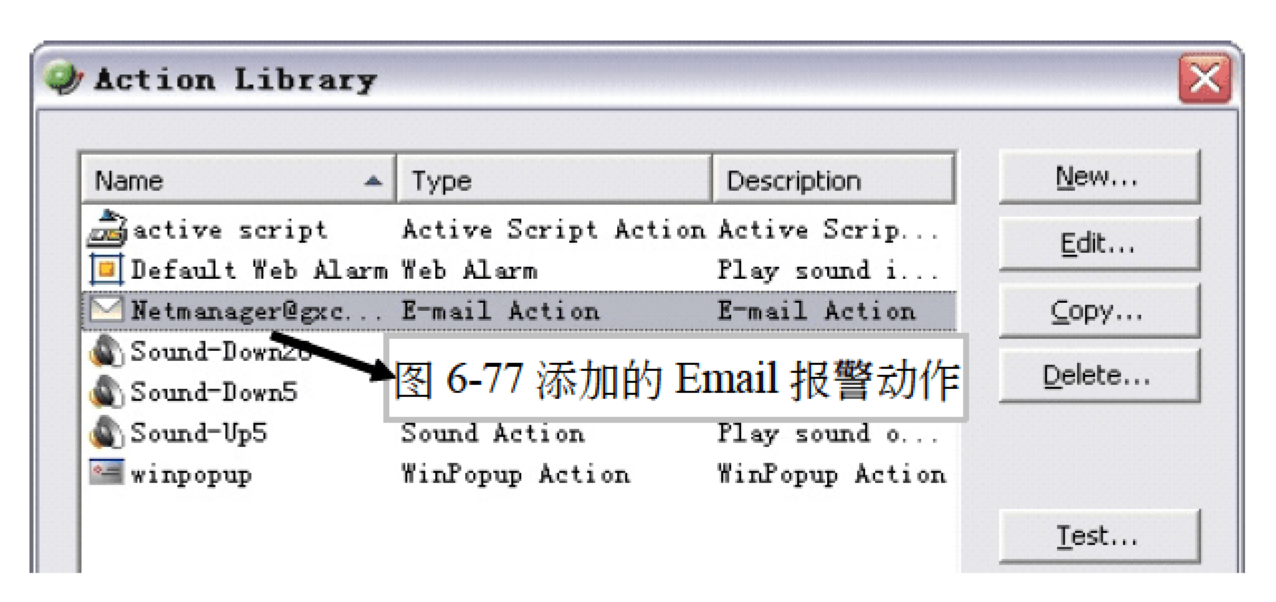


图 6-78　查看添加的 E-mail Action

图 6-79 中，展示了邮件报警提示方式中邮件内容的样式。

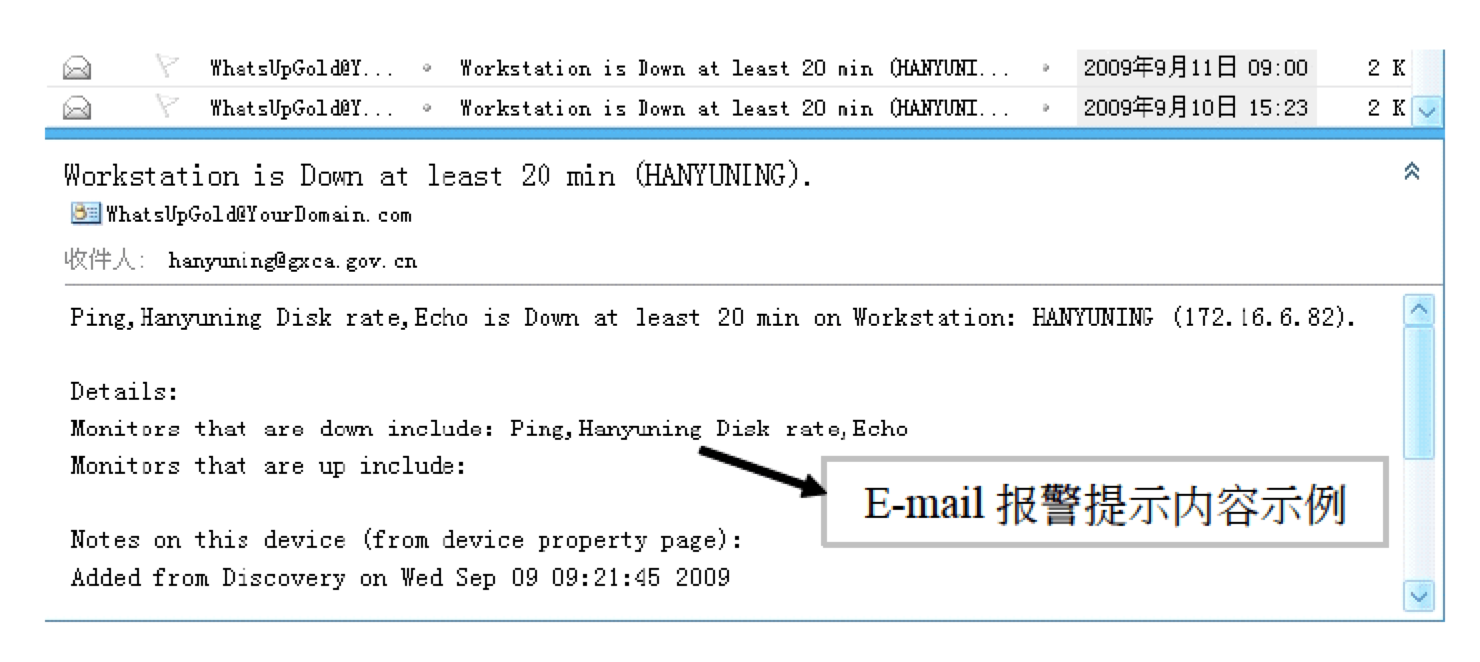


图 6-79　邮件提示的内容展示

报警提示的内容为：IP 地址为 172.16.6.82 的计算机中，Ping 服务无法连接、Echo 服务停止时间超过了 20 分钟、磁盘利用率超过了设置的阈值。

实例 2：添加 WinPopup Action

弹出消息提示框，首先需要开启计算机的消息服务。在控制面板中选择【服务】|【Messenger】选项，在设置框中，将该服务状态设置为开启状态，如图 6-80 所示。

开启服务后，回到 WhatsUp Gold 的 Action Library 界面，并单击 New 按钮来添加一个动作类型为 WinPopup Action 的报警动作，如图 6-81 所示。



图 6-80　开启 Messenger 服务

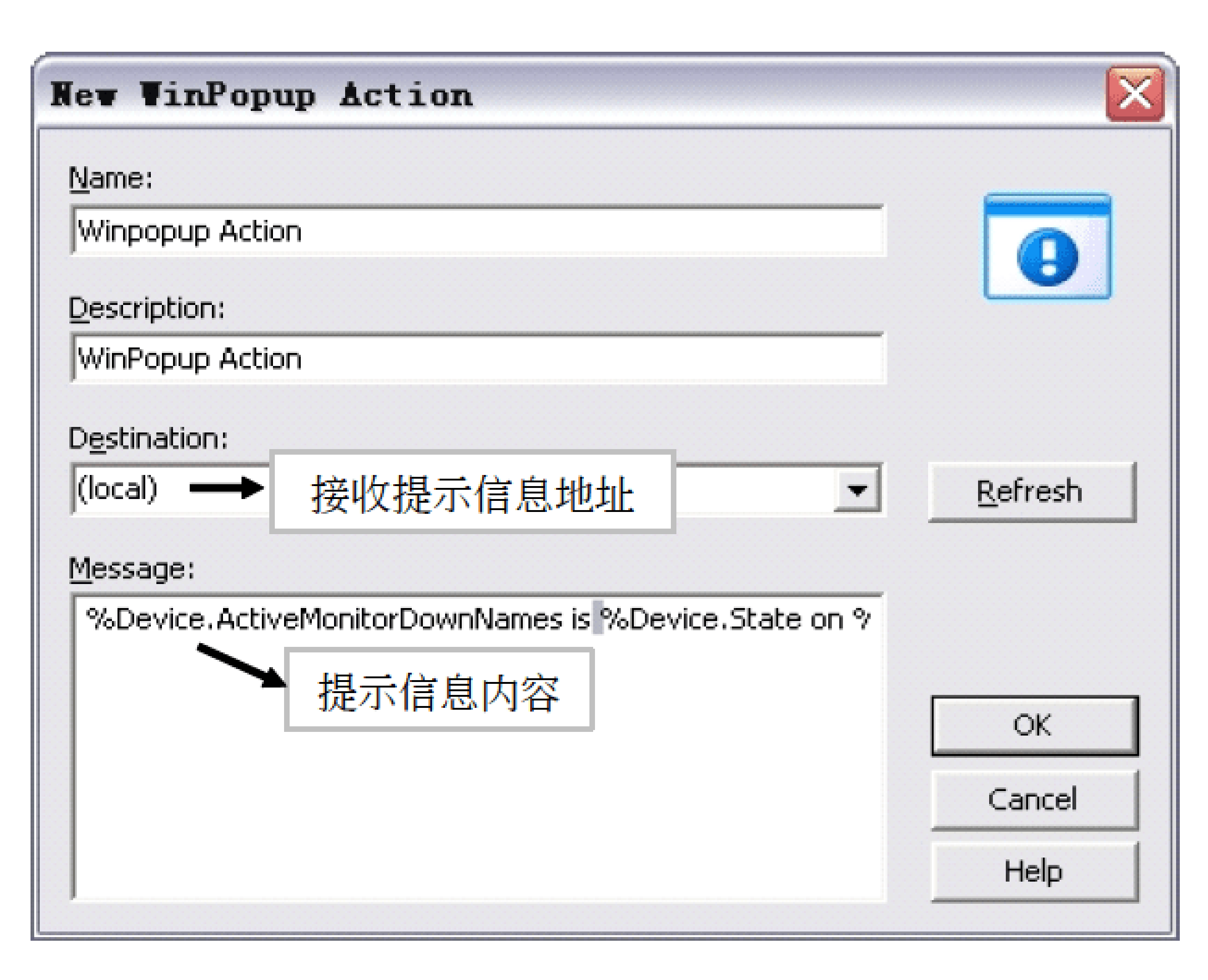


图 6-81　添加报警动作 WinPopup Action

在图 6-81 中，Message 文本框中设置的内容为弹出框的提示信息，需要输入带参数的语句。WhatsUp Gold 提供了多种参数，包括设备名称、IP 地址、监测项目名称等。在表 6.6 中，列出了 WhatsUp Gold 中提供的可用于设置提示信息的参数。

表 6.6　WhatsUp Gold 中提供的可用于设置提示信息的部分参数

设备参数名	描　述
%Device.ActiveMonitorDownNames	当设备主动监测项目停止服务并触发报警时，显示停止服务的对象名和停止时间。例如，Ping、DNS、 Echo 等服务停止至少 5 分钟
%Device.ActiveMonitorUpNames	当设备主动监测项目启动服务并触发报警时，显示启动服务的对象名和停止时间。例如，Ping、DNS、 Echo 等服务启动至少 5 分钟
%Device.DisplayName	显示设备的自定义名称
%Device.Address	显示设备的 IP 地址
%Device.State	设备状态的描述，如 Down at least 2 min
%Device.Type	显示设备类型，如 Workstation、Switch、Router 等
%ActiveMonitor.Name	主动监测项目的名称
%ActiveMonitor.State	显示监测项目当前状态，例如 Down at least 5 min.
%System.Date	报警发生时的系统日期
%System.Time	报警发生时的系统时间，格式为 hh:mm:ss

在设备发生故障时，管理员通常最关心的是发生故障的设备名、设备 IP 地址及发生了什么故障。所以在 Message 对话框中的语句包含以上几个关键参数即可，例如停止服务的主动监测项目名称、设备状态、设备主机名及 IP 地址等。参数语句描述示例如下：

```
"%Device.ActiveMonitorDownNames is %Device.State on %Device.Type:
%Device.HostName （%Device.Address）.
Details:
Monitors that are down include: %Device.ActiveMonitorDownNames
Monitors that are up include: %Device.ActiveMonitorUpNames
Notes on this device （from device property page）:%Device.Notes"
```

配置消息提示框参数完成后，可对该新建报警动作进行测试。测试结果如图 6-82 所示。



图 6-82　测试发送的报警消息

实例 3：添加 Syslog Action

使用该方式，WhatsUp Gold 可以把监测到的故障或状态信息按照需要的内容和格式（例如状态改变的 IP 和故障内容等信息），发送到指定的日志服务器上。如果要使用该功能，则需要在日志服务器上安装日志接收程序。推荐的日志分析软件为 Kiwi Syslog Daemon。该软件的使用将在本书第 11～12 章 Kiwi Syslog 部分进行讲解。

在庞大的网络中配置日志服务器很重要。发生网络故障时，不需要登录到每台网络设备中去查看日志，而只需要查看集中了所有网络设备的日志服务器，方便、易读、详细的日志信息便能够帮助你快速定位故障主机。同时，日志服务器能够保证日志的安全。假如

主机被入侵，入侵者可能会删除主机中的所有系统日志。而日志服务器可以把所有的入侵记录如实记录。

WhatsUp Gold 程序中同样支持 Syslog 功能，也支持将日志转储。WhatsUp Gold 通过默认端口 514 监听日志以及输出日志信息。在 Kiwi Syslog Daemon 程序中，默认监听端口包括 Tcp1468、Udp514、Snmp162，所以并不需要对日志接收软件做任何设置，就能够接收到 WhatsUp Gold 转储的日志信息。

以下介绍 Syslog Action 的配置。首先在 Action Library 中选择新建类型为 Syslog Action 的报警动作，并输入动作名称、接收日志的服务器 IP 地址及系统日志监听的 UDP 端口号（默认端口为 514），如图 6-83 所示。



图 6-83 添加 Syslog 报警动作

然后为某监测项目或主机添加该报警动作。产生报警信息后，查看日志程序 Kiwi Syslog Deamon，将看到由 WhatsUp Gold 发出的指定格式的报警信息，如图 6-84 所示。

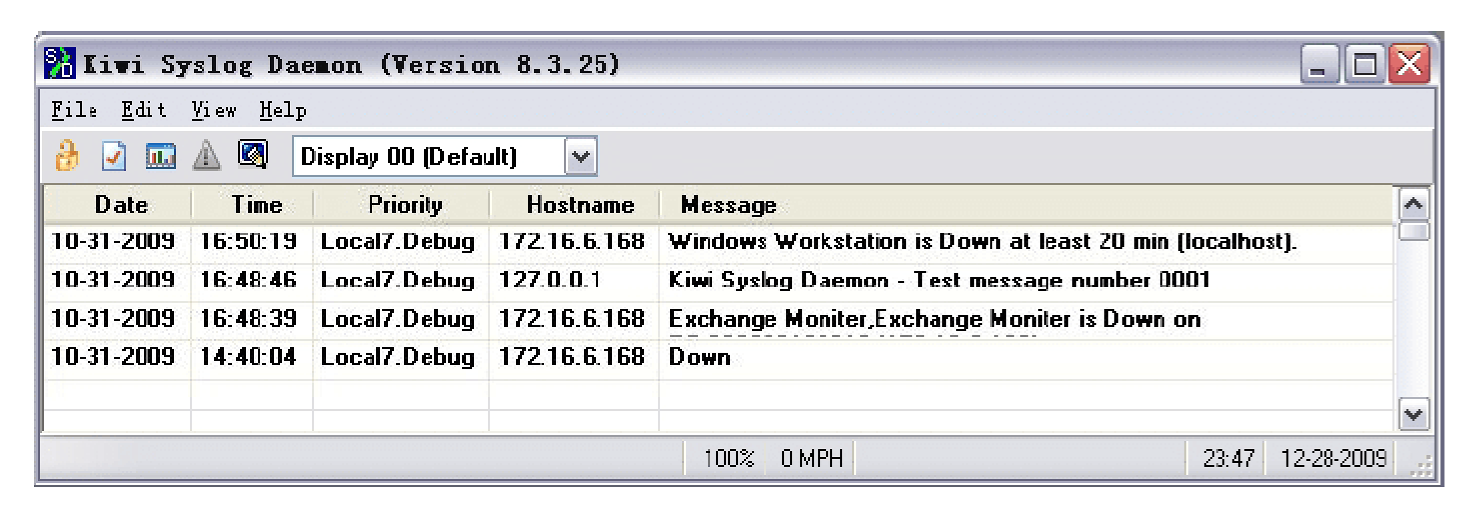


图 6-84 Kiwi Syslog 软件中接收的日志信息效果

实例 4：添加 Program Action

在 Action Library 界面选择新建提示动作类型为 Launch Program Action，发生报警时自动调用指定的外部程序。例如，监测 Web 服务器是发现 HTTP 服务停止，则调用 Wireshark（抓包分析工具）软件执行抓包分析的操作。选择动作类型如图 6-85 所示。

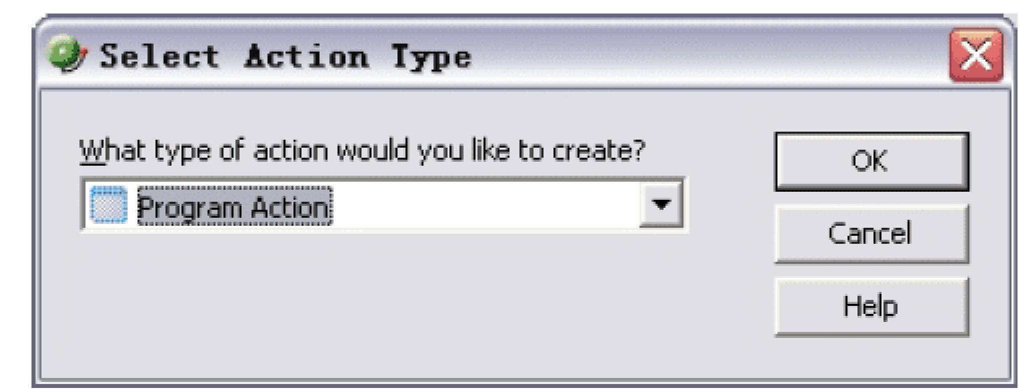


图 6-85 新建类型为调用外部程序的报警动作

选择 Program Action 后输入自定义名称，并在 Program filename 中选择需要调用的程序，在 Working path 选择存储外部程序执行结果的路径，在 Program arguments 文本框中输入需要传递给指定程序的参数，如图 6-86 所示。

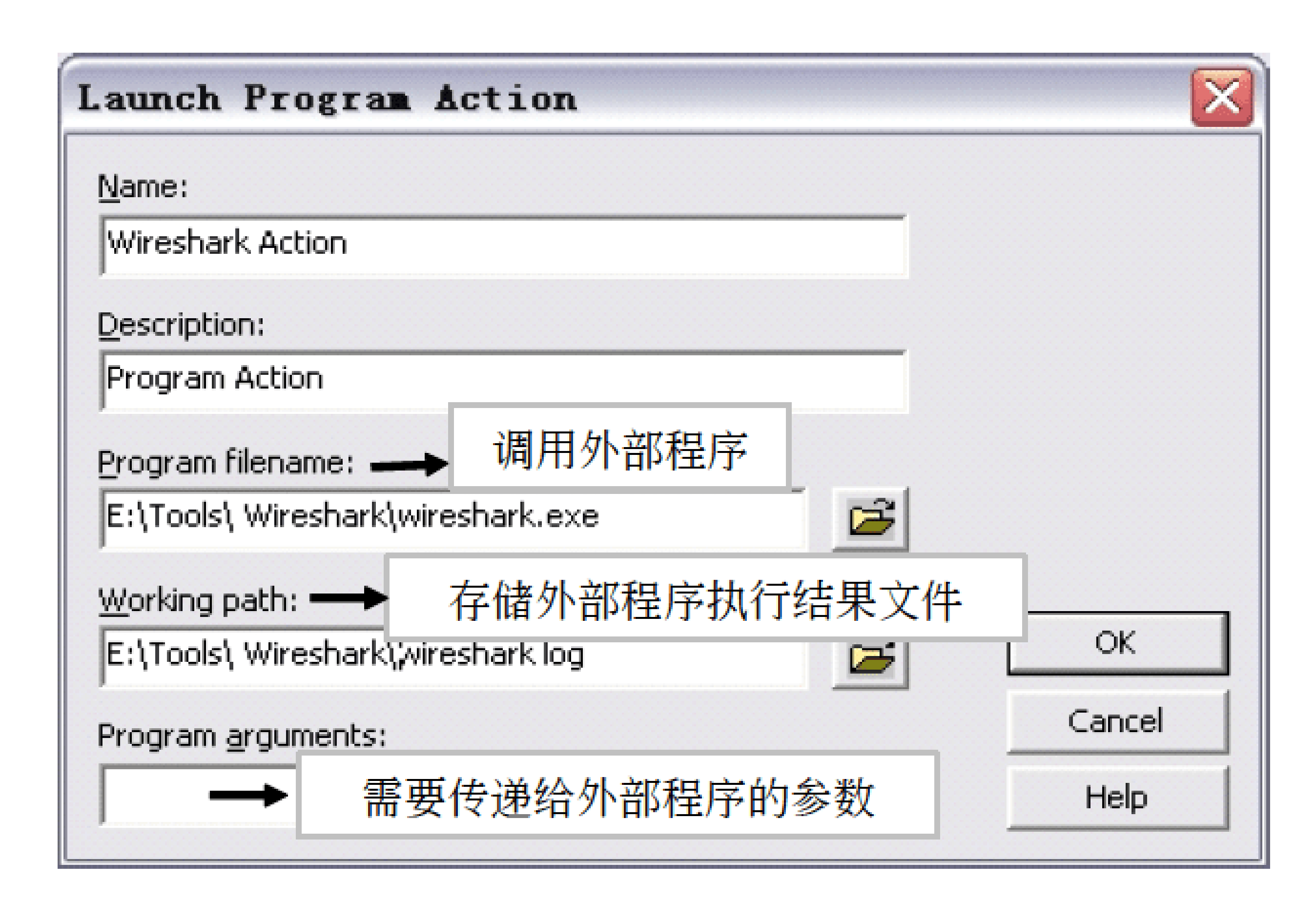


图 6-86 添加调用外部程序动作

实例 5：添加 Service Restart Action

Service Restart Action 可在系统状态变化时将远程主机上的指定服务启动或停止。例如，监测到远程 Exchange 服务器上发送邮件服务运行不正常时，直接重启 Exchange 主机上的 SMTP 服务。以下为添加重启 SMTP 服务的执行动作配置步骤。

（1）在 Action Library 中选择新建提示动作类型为 Service Restart Action，并在 Name 文本框中输入动作名。此例命名为 Restart SMTP Service。在 Host 文本框中选择要执行重启服务的主机对象，单击【...】按钮即可打开本地网络主机列表进行选择，如图 6-87 所示。

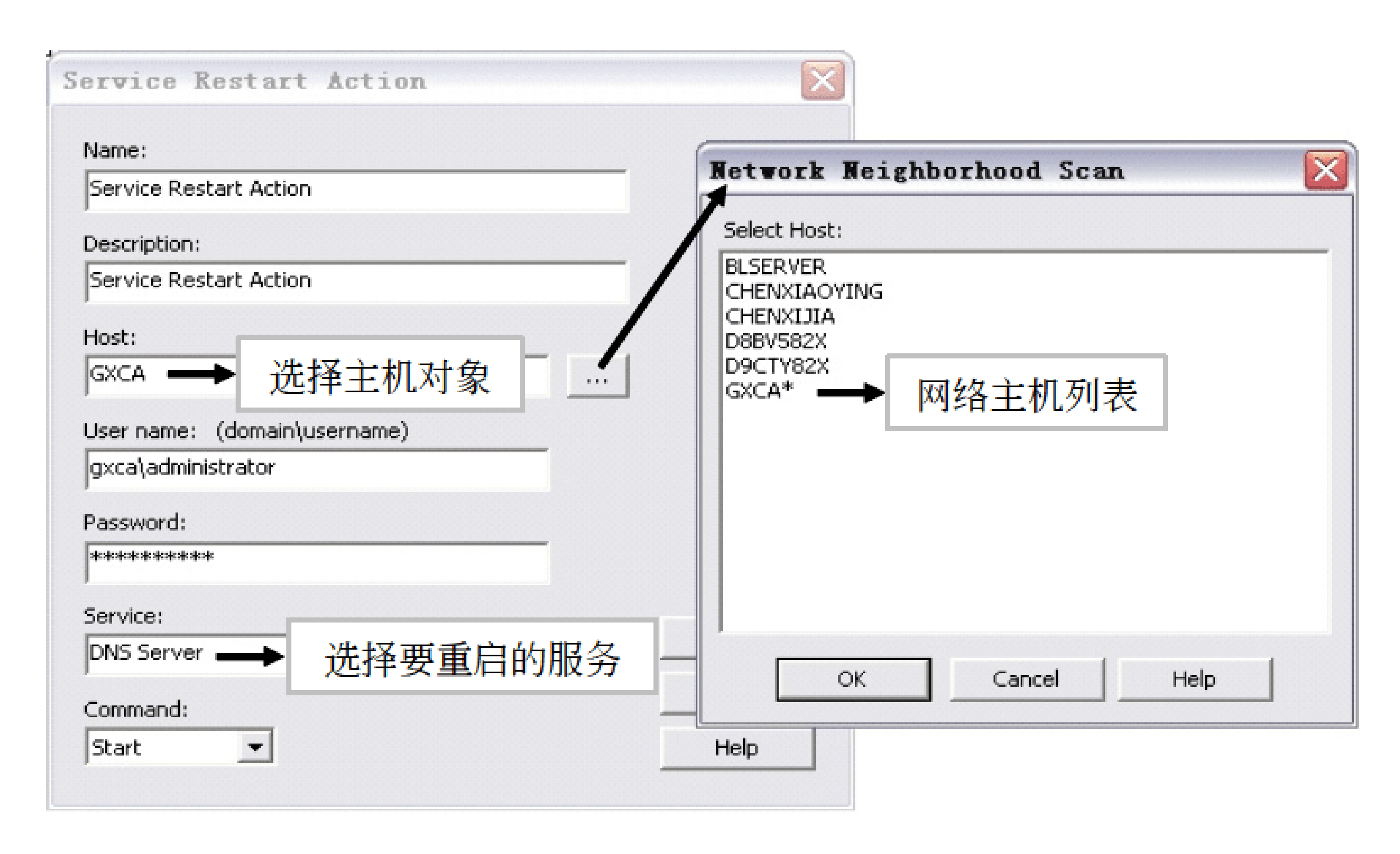


图 6-87 设置重启主机服务的动作

（2）在 User Name 和 Password 文本框中输入能正确的登录对象主机的用户名和密码，而且该用户名必须具有 Administrator 的管理员权限。如果该主机在 Windows 域中，则输入格式为“域名\用户名”；如果该主机在工作组中，则输入格式为“工作组名\用户名”或“机器名\用户名”；在 Service 选项中，列出了所选主机中的所有服务，包括正在运行和停止的服务（如图 6-88 所示）。该例中选择启动“SMTP”服务。

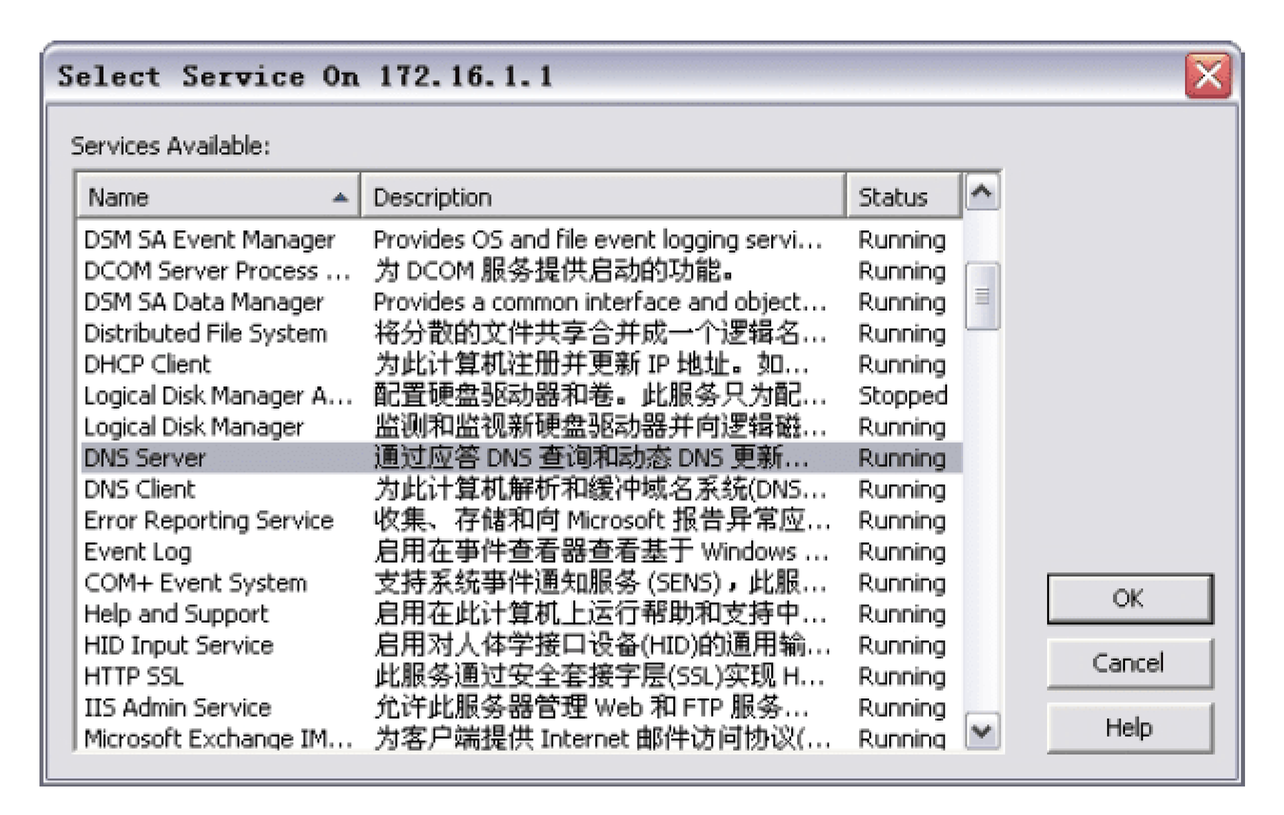


图 6-88　选择要重启的服务

（3）在 Command 选项中，可选择对远程服务做启动还是停止的操作。完成这些选项的配置后在 Action Library 中建立该动作。

6.3.3　配置动作策略

动作策略就是一系列报警提示动作的组合，为某设备新增动作策略比逐个为该设备添加个别动作要更简单快捷。同时，动作策略管理比一系列动作的列表更容易管理，也能够减少更多的工作量。

（1）选择主界面菜单 Configure | Action Policies 命令，打开策略库。在该界面中可对动作策略做新增、修改、复制和删除操作。此处单击 New 按钮新建策略，结果如图 6-89 所示。

（2）为该策略命名后，单击 Add 按钮可新增策略。在弹出的对话框中，提供了从动作库中添加动作或新建动作。前面已经介绍了如何新增动作，此处选择从库中添加动作，如图 6-90 所示。

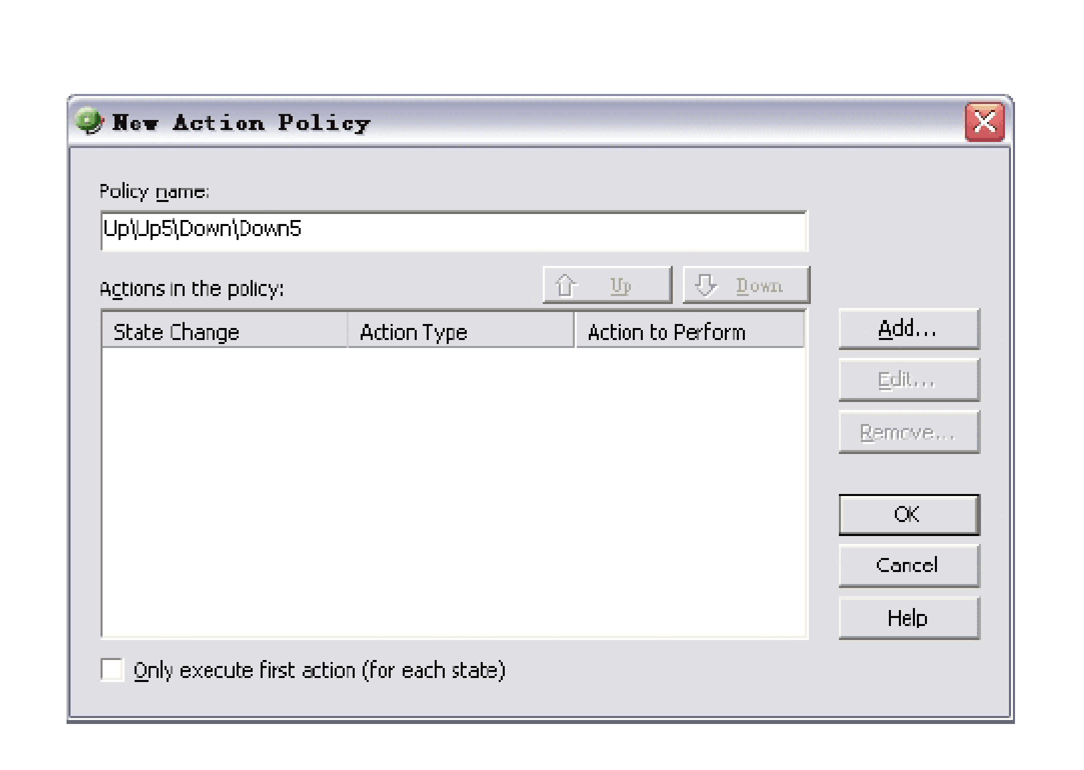


图 6-89　动作策略库

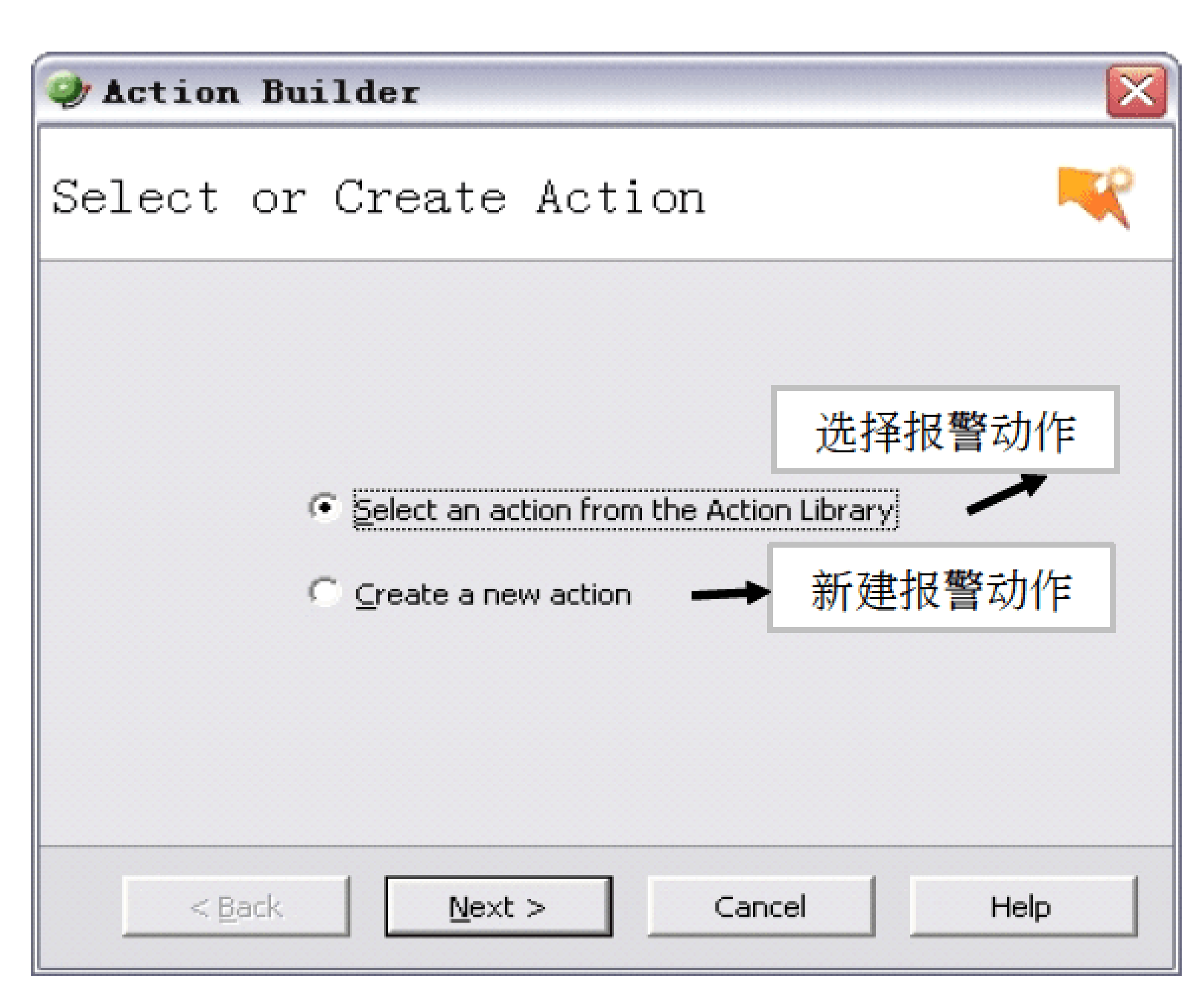


图 6-90　为策略选择动作成员

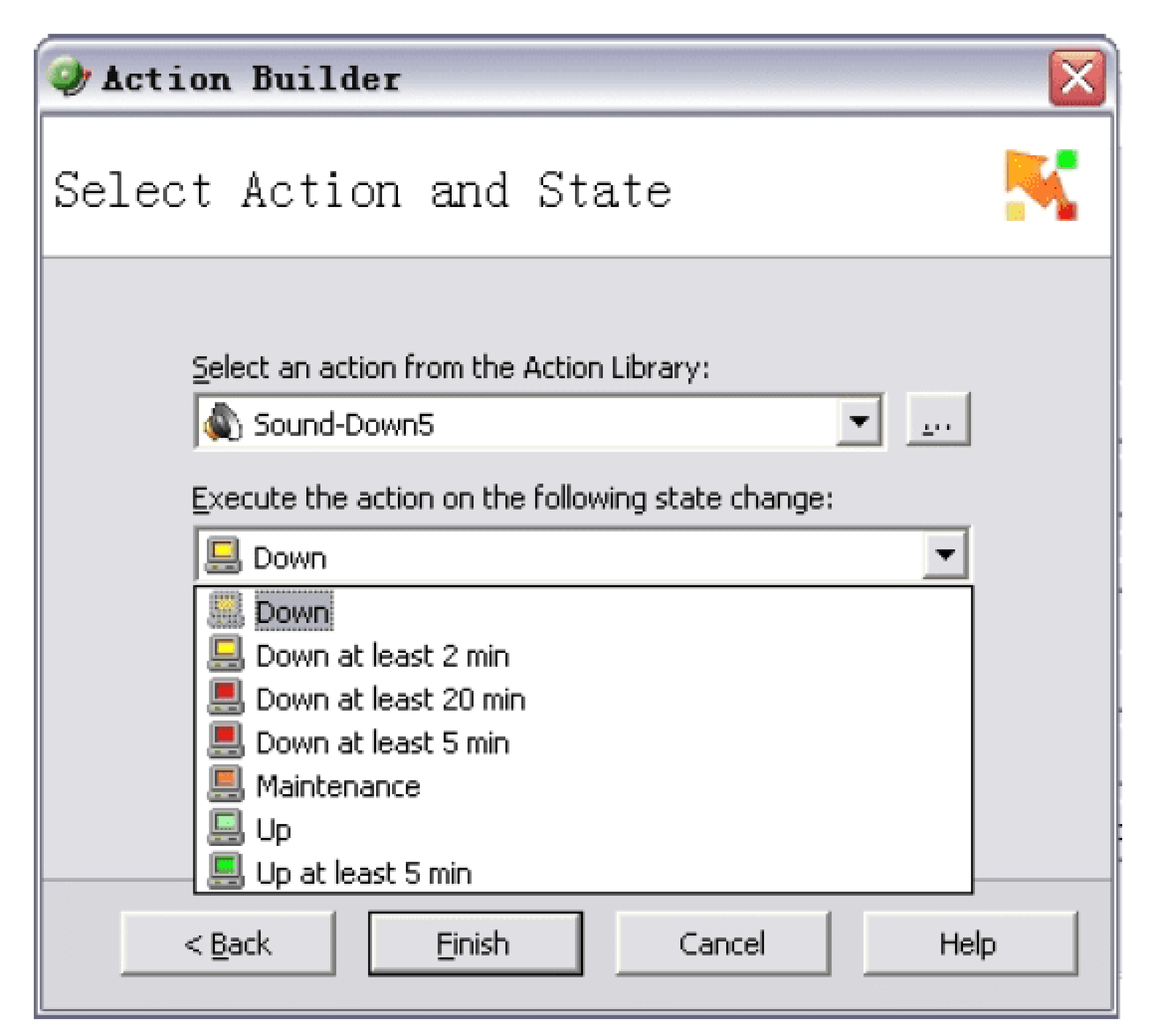
（3）本示例中，通过选择动作方式，建立报警策略，其中包括如下 4 个动作：

❑ 设备状态变为 Down 时，执行声音报警动作。
❑ 设备状态变为 Down 超过 5 分钟时，发送邮件作为报警信息的记录。
❑ 设备状态变为 Up 恢复正常运行时，执行声音提醒。
❑ 设备恢复正常运行超过 5 分钟后，认为运行已稳定，发送日志作为记录。

同时，配置执行声音提醒的时间段为：周一至周日的 6:00PM～08:00AM，也就是仅允许在上班时间发出声音提醒。

首先，添加设备状态为 Down 的声音报警。在动作库下拉列表中，选择 Sound-Down5 的声音报警。此处的 Sound-Down5 或 Sound-Down20，区别仅在于执行的声音文件不同。在下方动作状态改变执行动作的下拉列表中选择 Down，即在设备状态由 Up 变为 Down 的时刻，马上执行声音报警，如图 6-91 所示。

对第 1 个声音动作，还需要配置不执行的时间段为周一到周日的 6:00PM～8:00AM。单击 Blackout Schedule 按钮，打开停止动作的日程管理界面，然后单击 Add 即可添加日程，如图 6-92 所示。





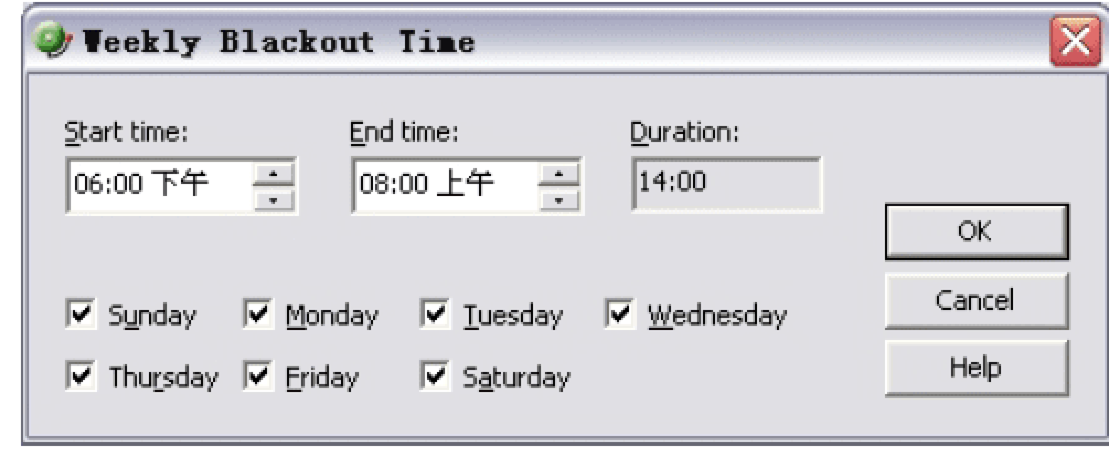


图 6-91　设备 Down 时执行声音报警

图 6-92　设定不执行声音报警的时段

（4）添加第 2 个动作。再次单击 New 按钮，并添加当设备状态变为 Down 且超过 5 分钟时，发送邮件提示的动作。在动作库下拉列表中，选择执行发送邮件。在动作状态变化类型下拉列表中选择 Down at least 5 Min，即设备 Down 超过 5 分钟后，发送邮件至指定邮箱，如图 6-93 所示。

（5）添加第 3 个动作。单击 New 按钮，并添加当设备状态变为 Up 时执行声音提示。添加方式如第三步骤。

（6）添加第 4 个动作，即在设备恢复正常运行超过 5 分钟后，向日志服务器发送日志信息，如图 6-94 所示。

（7）至此，添加了该 4 项在不同时刻执行的报警动作。可以看到，在该策略的动作列表中已经包含了添加的 4 个动作，如图 6-95 所示。

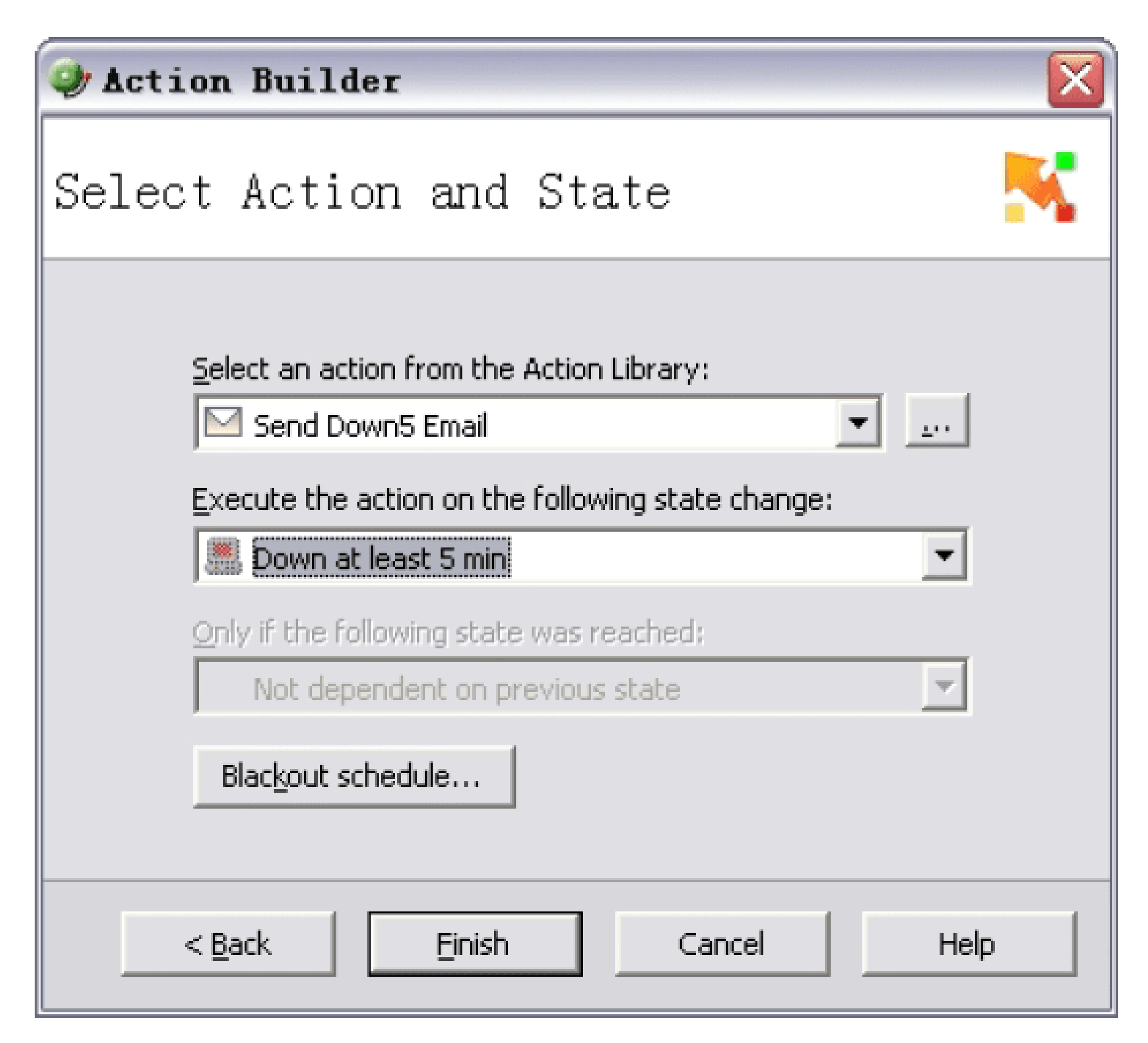


图 6-93 设备 Down 超过 5 分钟，则发送邮件提醒

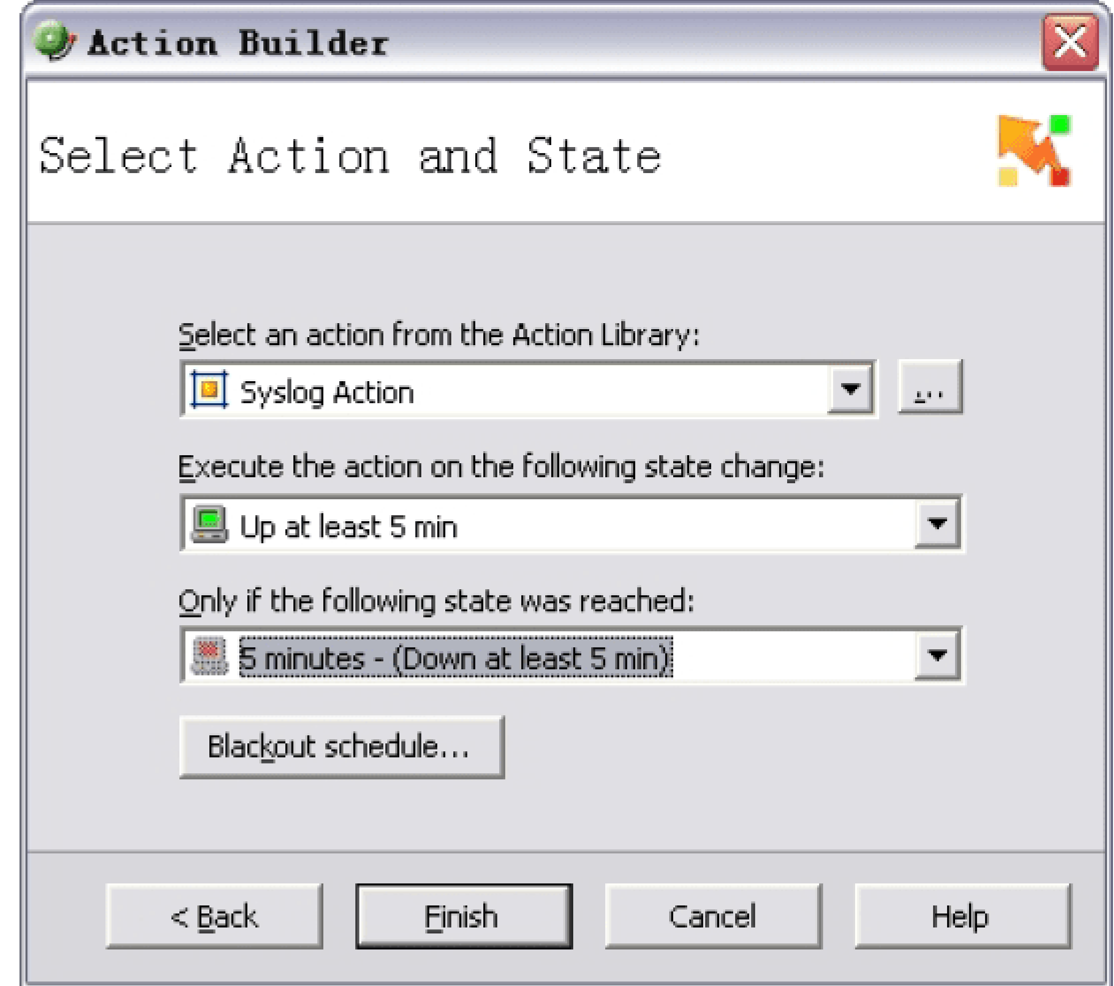


图 6-94 设备 Up 超过 5 分钟，发送日志作为记录



图 6-95 新建策略中包含的 4 个动作

注意：（1）大量的设备存在发送出大量报警提示信息的可能（如 Email、短信、提示音等）。如果一个报警提示动作设置在一台路由器上，而大量的设备和监测内容都依赖该路由器连接到互联网，则当路由器出现故障停止运行时，路由器后方的所有设备都被显示为关闭（无法连接），那么每台设备均会发出报警信息。该情况可考虑使用依赖关系以及对路由器和其他重要网络设备做报警提示的限制。

（2）声音报警提示方式适合于在设备附近实时有人值守，较容易听到声音报警的环境下。但声音提醒方式不适用于夜间值守设备。

（3）报警动作可以添加至设备本身和监测项目。如果对某个设备同时添加了设备报警提示和监测项目报警提示，那么当监测项目发生报警时，设备也认为出现故障也发出报警提示。

6.3.4 为监测内容增加报警动作

配置了各种报警提示动作及动作策略后，可根据需要为设备和监测项目添加动作或者策略。在设备属性中，可以为如下 3 类项目添加报警动作，如图 6-96 所示。

- ❑ 为主动监测项目添加报警提示动作或报警策略。
- ❑ 为被监测项目添加报警提示动作（无法添加策略）。
- ❑ 为设备的运行添加报警提示动作。

1. 为监测项目添加报警策略或动作

选择某设备，打开其属性界面，选择 Active Monitors 页面，该页面列出为该设备添加的主动监测项目列表。在列表中选择某一监测项目，然后双击该项目（例如选择 HTTP），在弹出的属性窗口中可为该 HTTP 监测项目添加报警动作，如图 6-97 所示。



图 6-96 监测项目类型

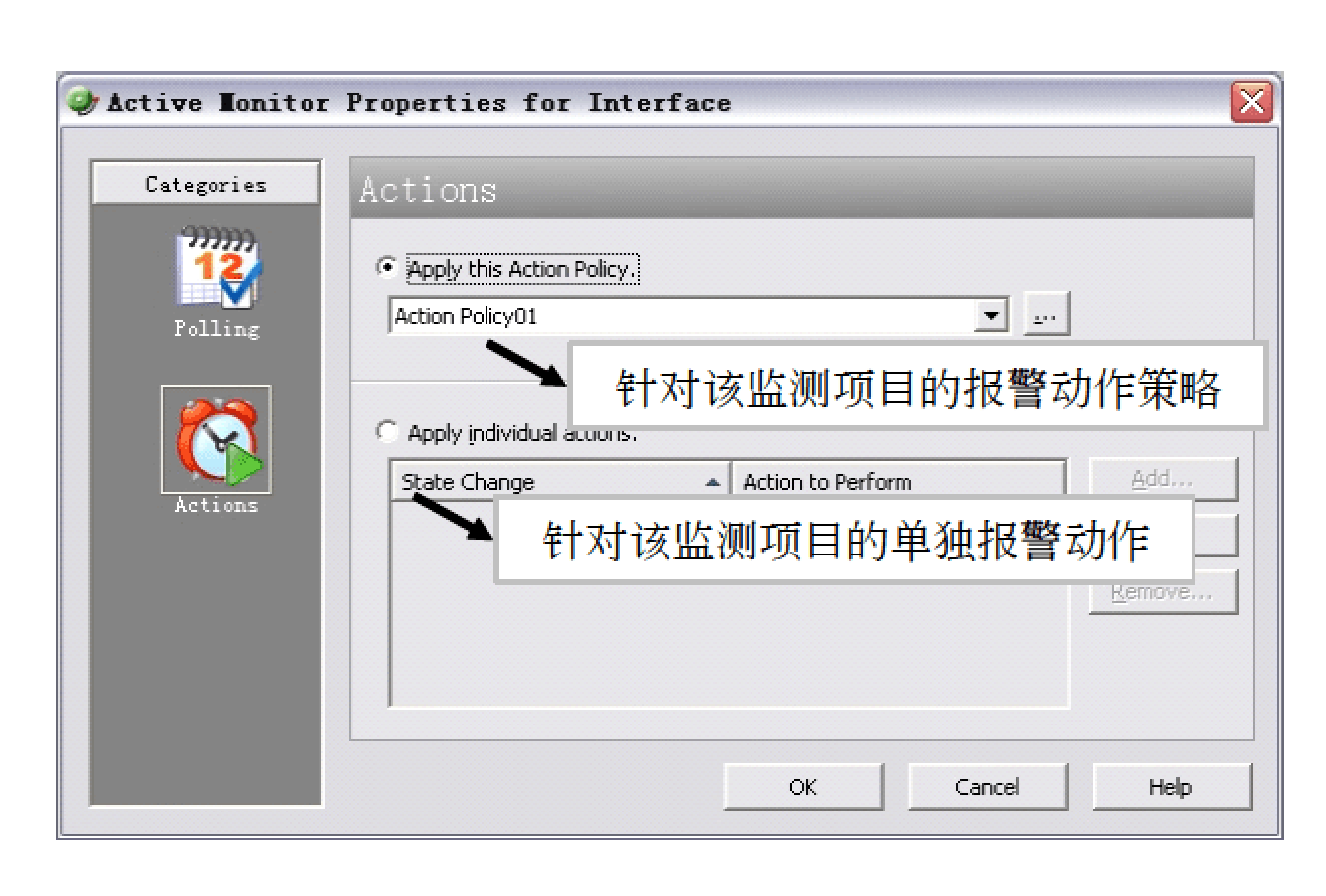


图 6-97 为监测项目添加报警动作

2. 为设备批量添加报警策略

在设备列表中可同时选择多个设备，并为这些设备添加报警策略。选择多个设备后，右击打开快捷菜单，并选择 Bulk Field Change | Action Policy 命令，然后在弹出的对话框中选择策略即可，如图 6-98 所示。

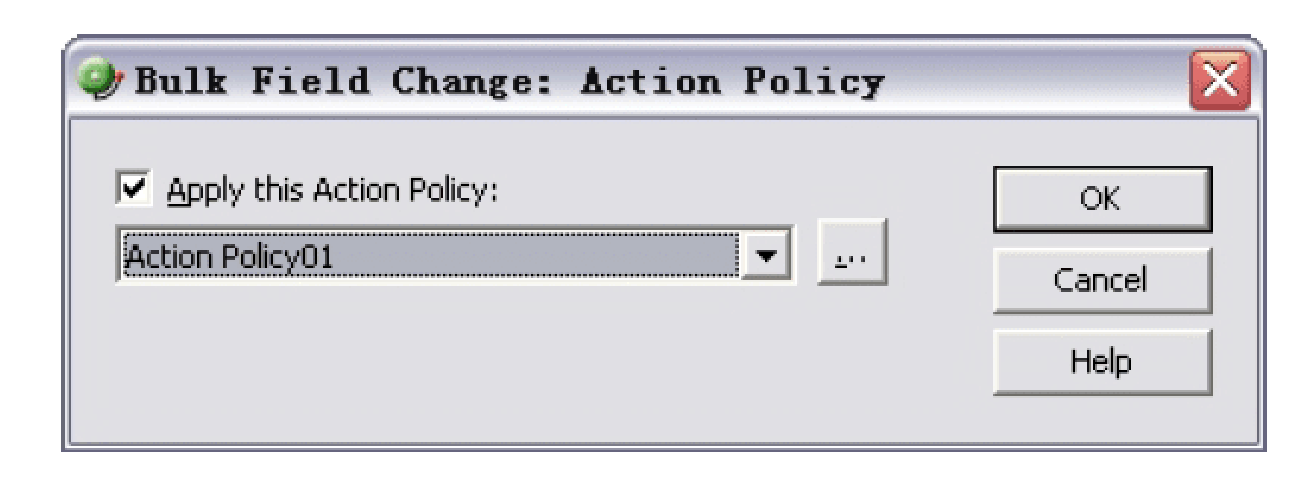


图 6-98 批量添加报警策略

6.4 Map View 拓扑视图配置

SNMP 设备扫描结束后，在 WhatsUp Gold 主界面的 Map 视图中将会显示每次扫描生成的设备组中的所有设备图标。可以根据需要配置拓扑图以展示网络结构，以及设备之间和子网之间的关系结构，如图 6-99 所示。

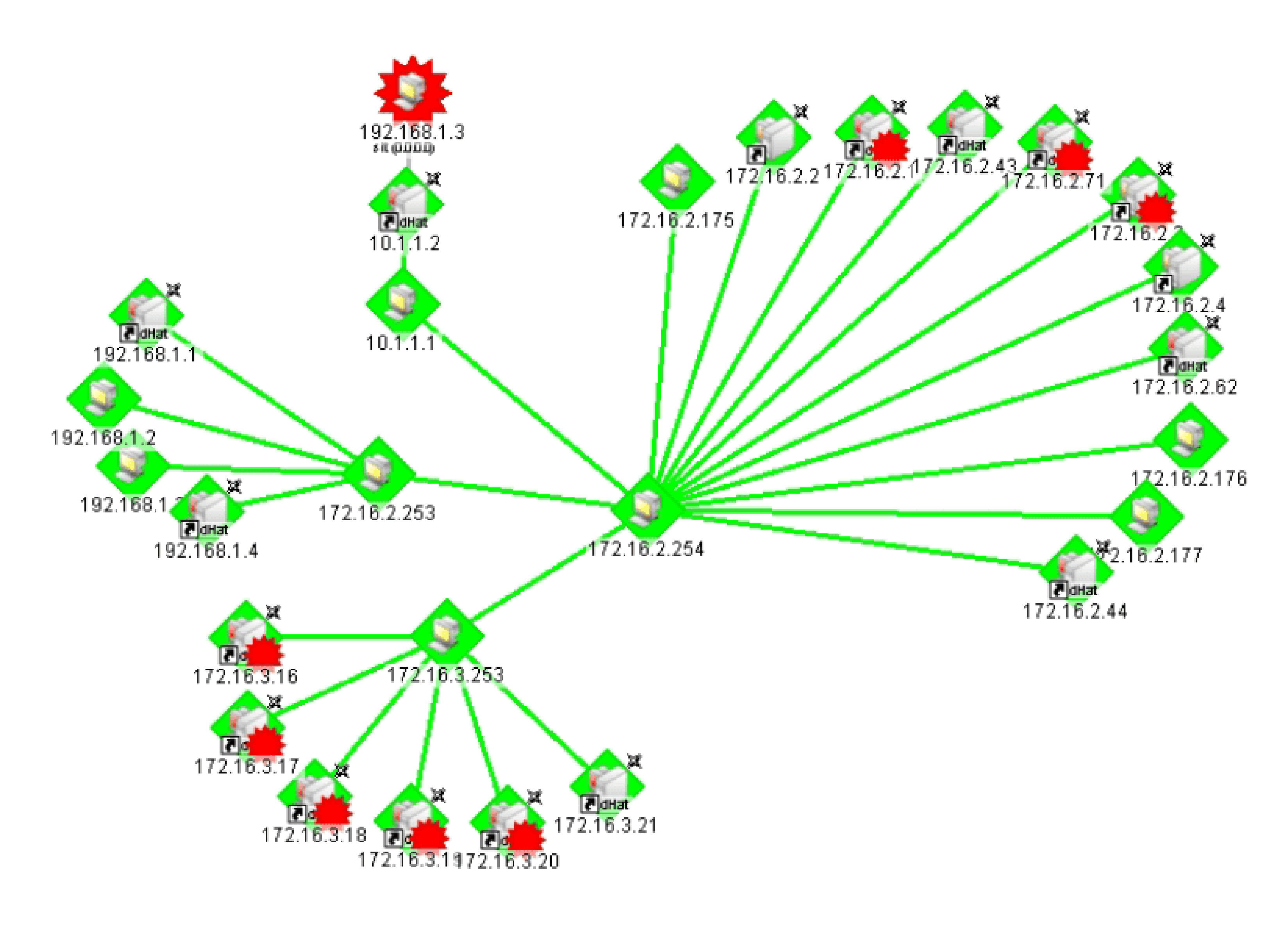


图 6-99　网络拓扑视图

6.4.1 Arrange 菜单命令和图标栏简介

1．Arrange 菜单命令简介

进入 Map 视图中，主菜单将会多出一个主菜单命令 Arrange，用于对设备做调整和布局，如图 6-100 所示。

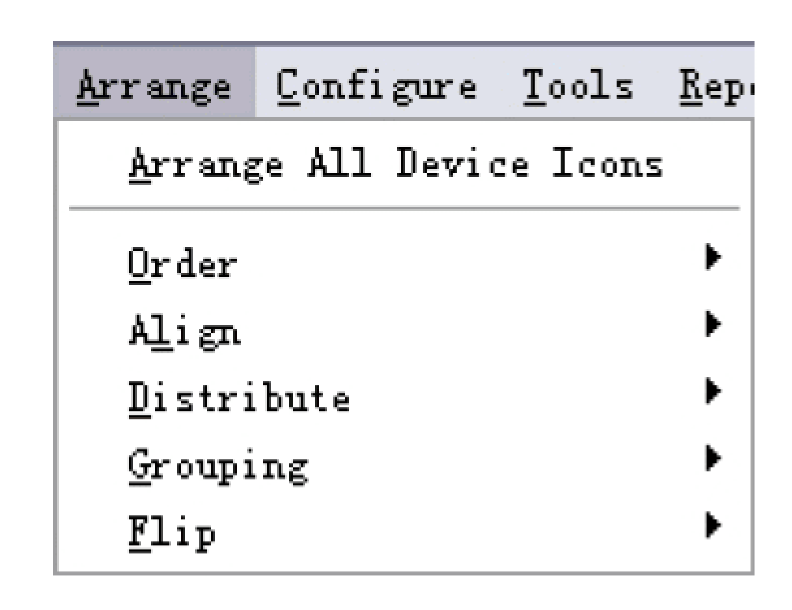


图 6-100　Arrange 菜单命令

- ❑ Arrange All Device Icons：能够重新整齐排列视图中的所有设备。首先在 Map 视图中通过拖动全选所有设备，然后选择菜单命令 Arrange | Arrange All Device Icons 即可重新排列所有图标。
- ❑ Order：排序命令。该菜单命令可改变图标的显示层次，使图标至于最前面或最后面。
- ❑ Align：对齐命令。能够参照第一个图标位置对所有图标进行排列对齐。
- ❑ Distribute：布局命令。重新对图标进行布局，使其间隔均匀等。

- ❑ Group：组合命令。能够将选择的“注解”元素组合，其移动位置时将作为一个整体移动（注解是指在图标栏中提供的直线、圆圈、文字等用于注解的元素。
- ❑ Flip：交换命令。转换所选的两个注解的位置。

2．图标栏简介

如果需要更详细的描述网络和设备，那么可使用图标栏中的注解功能（包括直线、文字、圆圈、云图等），方便地在 Map 视图中添加图形或者图片，如图 6-101 所示。

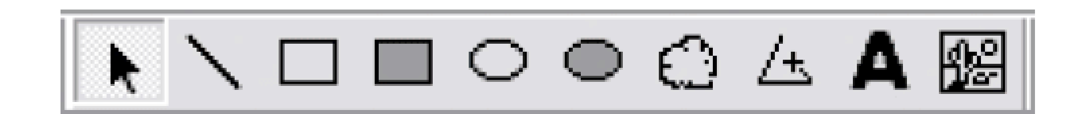


图 6-101　Map 视图注解

在添加完注解后，如果需要修改该注释的背景或边框颜色，可在该图形上选择右键菜单命令 Properties，改变图形的填充色、边框色等。

6.4.2　Map 视图应用

1．使用链接线

在视图中，可以使用链接线将设备连接起来，以显示设备的连接关系。同时，链接线还能展示主动监测的服务项目状态。如图 6-102 所示为各种链接线的图标。

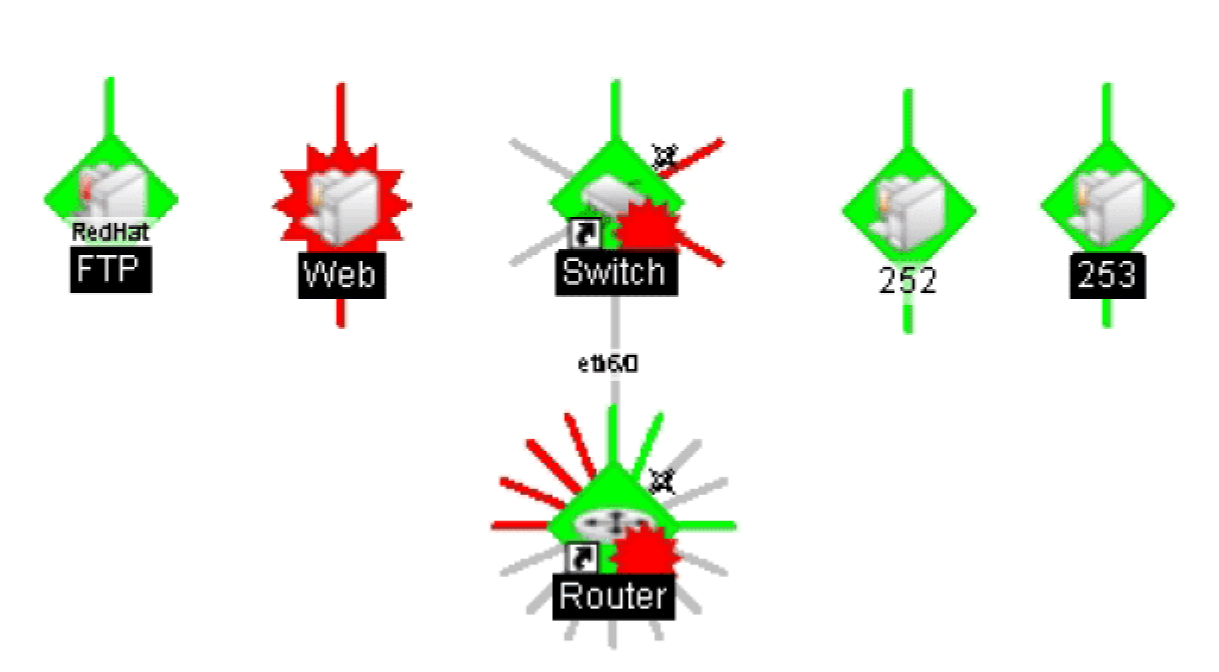


图 6-102　Map 视图中的各种链接图标

- ❑ Router1 显示的图标展示了路由器连接 RRA 服务器的连接状态为 Up，同时显示了该路由器还有 8 个无连接对象的接口，其中有一个连接状态为停用。
- ❑ 服务器 JMA 显示了该设备的两个连接状态均为 UP，包括 Ping 和 FTP 服务。
- ❑ 服务器 RRA 中的 FTP 服务状态为 Down，该服务器共有 5 条连接，其中两个为停用的。

也可以通过链接线颜色简单判断其状态。绿色表示该设备的一项服务状态为 UP；红色表示服务状态为 Down；橘红色表示该设备正处于维修状态中。

2．创建连通的链接线 Link Line

WhatsUp Golda 共提供了 3 种建立设备连接的方式。

方式1：在Map视图中，选择某设备并打开快捷菜单，选择Link | Link to命令，将弹出提示框，如图6-103所示。

在弹出的提示框中，列出了该设备上的物理接口和提供的服务对象（也就是主动监测的服务对象）。选择需要通过连接来显示其状态的服务对象，此处选择Ping服务，如图6-104所示。

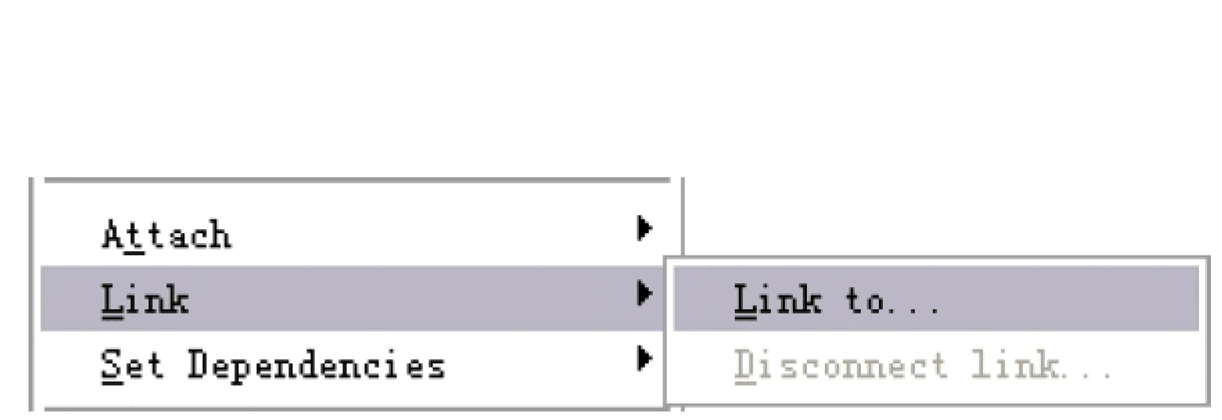


图6-103　添加能够显示状态的连接

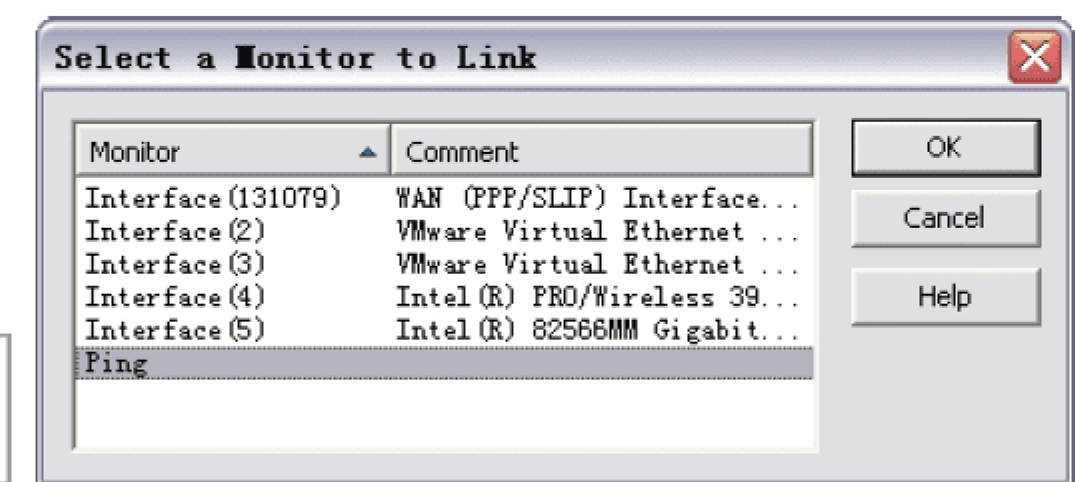


图6-104　设备接口及提供的服务对象

单击OK按钮后，将在该设备图标上显示箭头图标。然后选择需要连接的目标主机，即可建立设备间的链接线，即所选设备通过Ping方式连接至目标主机。如果两台设备之间Ping正常，那么连接会显示为正常的绿色。

如果要删除该设备到目标主机的连接，可选择该设备并右击，在弹出的快捷菜单中选择link | Disconnect link命令，即可删除连接。

方式2：为自动发现方式。在扫描发现设备的时候，选择SNMP Smartscan方式，同时在扫描选项中必须包含接口服务项。

方式3：为自动发现方式。选择某设备并打开其属性，然后选择Active monitors页面，然后单击Discover按钮，将自动发现该设备接口及其可监测对象，如图6-105所示。

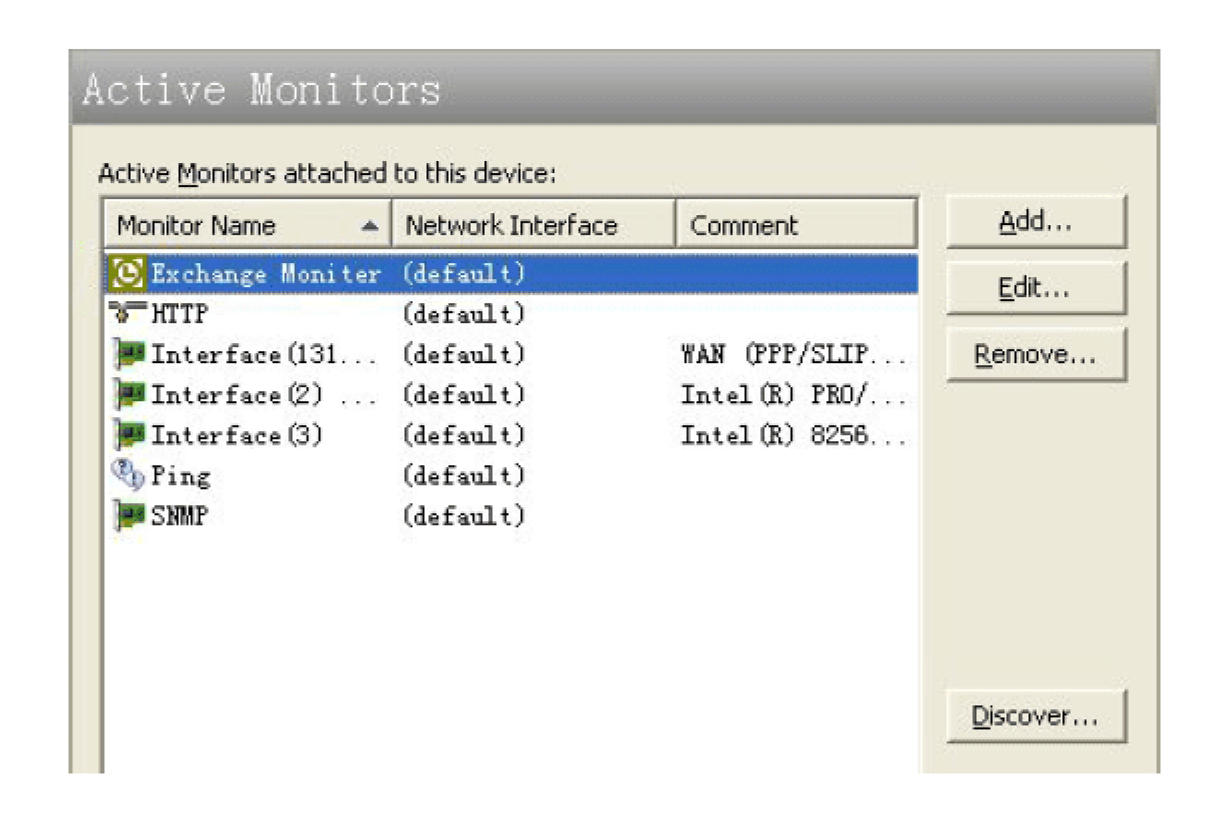


图6-105　Discover自动识别设备端口

注意：（1）当选择通过SmartScan自动发现方式，在扫描设置中需要输入路由器或交换机等网络设备正确的Community string，使扫描能够识别网络的接口信息。同样，在设备属性的主动监测项目中选择Discover，同样需要在Credentials中输入正确的Community String。

（2）手动方式为设备创建连接时，如果所选的服务没有连接对象而无法连通，那么连接将变为无法显示服务状态的普通连线。

（3）显示限制。默认WhatsUp Gold能显示256台以下的设备。可以通过修改注册表选项，使其能显示更多的设备。在注册表中找到HKEY_LOCAL_MACHINE\Software\Ipswitch\Network Monitor\WhatsUpProfessional\2007\ Settings，然后更改MapView-MaxDevices的键值为大于256的数值即可。

3. 使用附加线 Attach Line

附加线展示了网管员主动为设备添加的连线，并能够跟随设备的移动而改变位置。这类线只用于用户自定义的直观显示方式，可添加于任何两个设备之间，但并不能展现两个设备的真正关系。设备间的真正关系的体现是通过 Link 线来展示的。

添加方式与添加 Link Line 方式相似，同样选择某设备右击，并选择菜单命令 Attach | Attach to…，选择对端设备后即完成附加线添加，如图 6-106 所示。

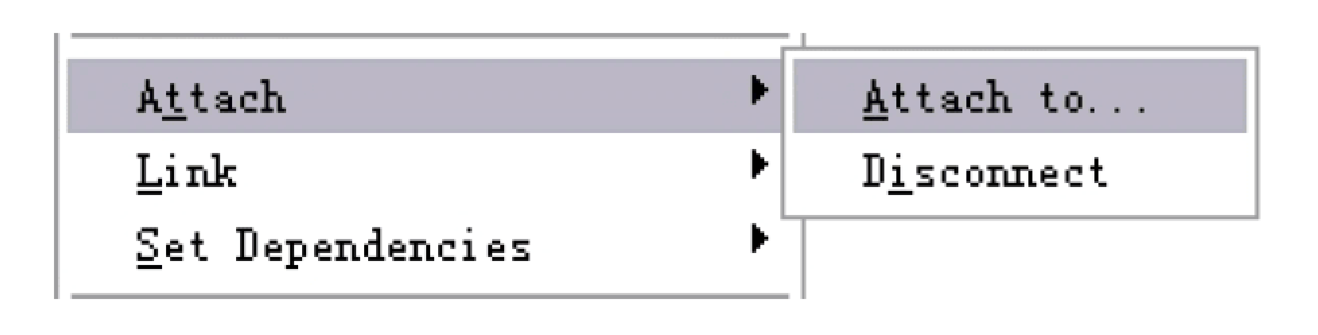


图 6-106　附加线

6.4.3　Map 视图右键菜单命令简介

Display 菜单命令可以改变设备的显示方式。在 Map 视图中右击，打开右键快捷菜单，如图 6-107 所示。

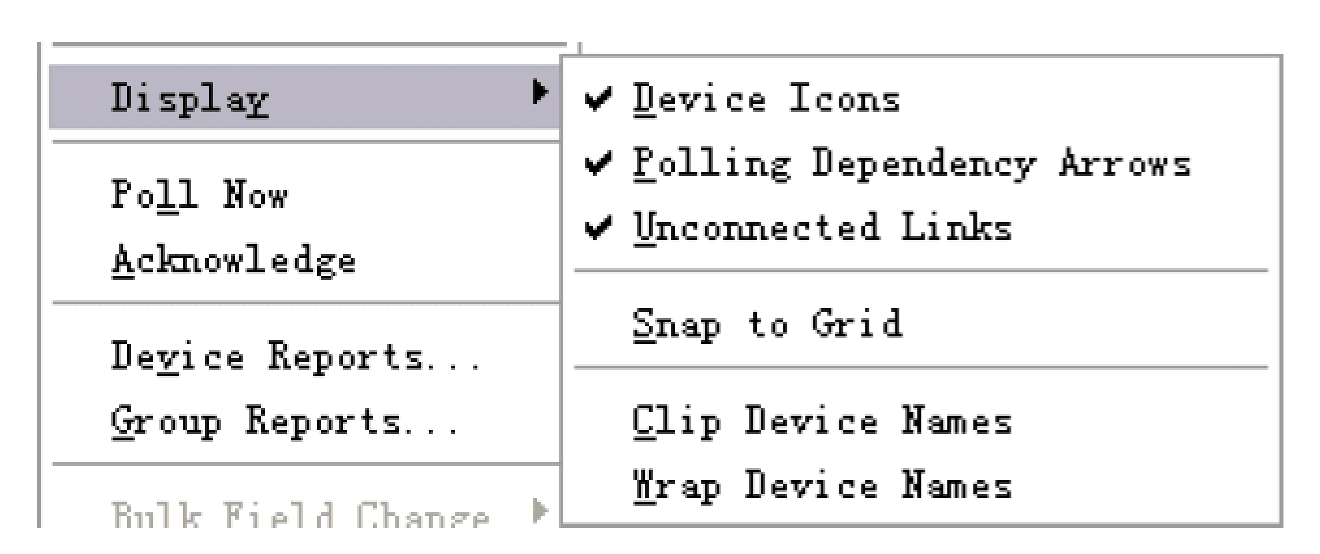


图 6-107　Map 视图中的 Display 菜单命令

在 Display 菜单中可做如下选择：

- ❑ Device Icons：选择该项，将会显示设备图标。否则将设备显示为小圆点的节点图标。如果设备数量较多，则以小圆点方式显示，会使视图更简洁。
- ❑ Polling Dependency Arrows：如果在设备间设置了依赖关系，对某设备的轮询需要根据另一个设备 Up 或 Down 的状态来决定，选择此项，将会显示设备间依赖关系的箭头。例如，如果设备 A 依赖于设备 B 的状态，那么将显示从 A 设备到 B 设备的箭头。
- ❑ Unconnected Links：选择此项，可以在视图中以短线的方式显示无连接对象的设备连接，其中包括设备接口和所有的主动监测对象。绿色表示状态为 Up，而红色表示 Down。
- ❑ Snap to Grid：选择此项，将在视图中显示网格并对齐在网格上。
- ❑ Clip Device Names：选择此项，将去除设备名称的域名部分，而仅显示设备的主机名。
- ❑ Wrap Device Names：选择此项，将以换行的方式显示设备的名称。

注意：如果需要固定某设备在视图中的位置，可在该设备上右击，选择 Lock Position 命令，如果需要重新移动设备位置，再次选择 Lock Position 菜单命令，将取消对设备位置的锁定。

6.5 本章小结

本章主要介绍扫描发现网络设备的方法、设备属性的详细配置，以及报警提示动作的功能和配置。通过本章学习，网管员应能够针对网络的实际情况使用合适的方式将所有网络组件纳入到程序监测中，并针对实际情况建立相应的报警提示动作。

第 7 章　网络设备信息采集和状态监测

在介绍了 WhatsUp Gold 的主要功能，包括扫描查找设备、配置报警动作和动作策略、设置各项属性及配置之后，本章通过实例介绍如何实现网络信息的采集和网络状态的监测。信息采集部分，通过实例分别讲解采集 Windows 系统、Linux 系统基础信息和网络设备基础信息；状态监测部分，通过实例讲解了 3 种监测方式。

- 性能监测：通过实例介绍机房温度、UPS、SQL 服务等监测。
- 主动监测：包括采用 WMI 方式监测非法入侵、SNMP 方式监测邮件服务器等。
- 被动监测：包括 Trap 方式监测，对系统日志、事件日志的被动监测等。

通过本章的实例应用介绍，能够使网络管理员将 WhatsUp Gold 程序熟练应用到实际工作中。

7.1 Performance Monitors 信息采集

本节介绍在 WhatsUp Gold 中，通过 Performance Monitors 方式采集 Windows 系统、Linux 系统和网络设备的基本信息，采集内容包括 CPU、磁盘、内存等硬件参数及其状态。

7.1.1 Windows 系统信息采集

此处选择在 Windows XP 操作系统中采集硬件基本信息，包括 CPU、Disk、Memory、Interface 的利用率等信息。操作过程如下：

首先在 WhatsUp Gold 主界面设备列表中选择一个 Windows XP 设备，并打开该设备属性界面。

在属性界面中，查看凭证 Credentials 页面选项，此处通过 SNMP 方式获取硬件性能信息，所以在 Credentials 页面添加 SNMP 认证字符串。按照该 Windows XP 主机中实际设置的 SNMP 读认证字符串，添加一个访问该主机的 SNMP V1 或 V2 类型的凭证。

添加凭证后，选择 Performance Monitor（性能监测）页面。默认在该界面列表中列出了 WhatsUp Gold 提供的 5 种硬件信息供采集，如图 7-1 所示。

双击 CPU Utilization 选项或单击该选项再单击 Configure 按钮，即可查看该 Windows 操作系统中的 CPU 信息，可看出该主机为双核 CPU，品牌为 Intel，如图 7-2 所示。

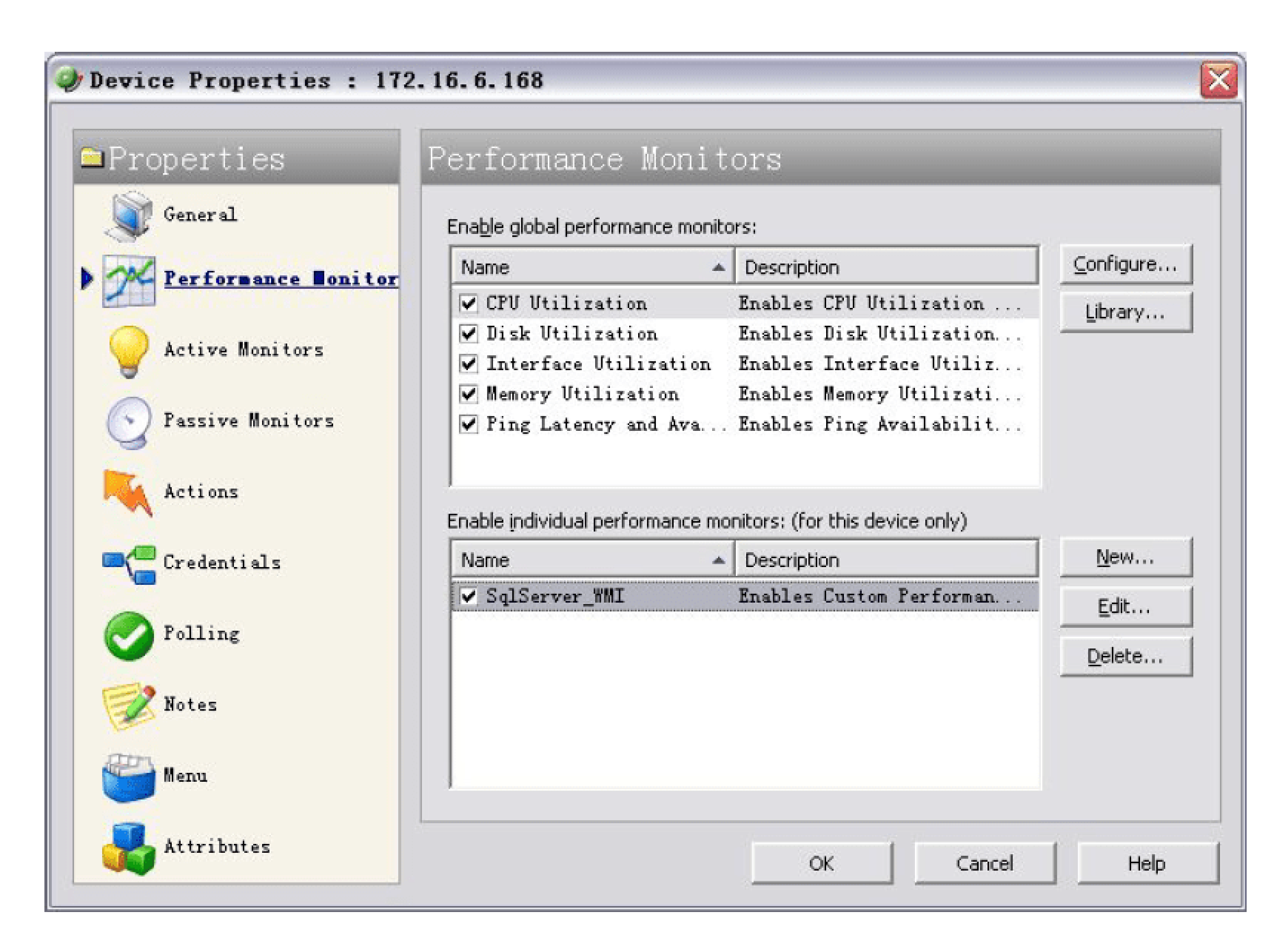


图 7-1 打开性能监测属性——采集基础信息

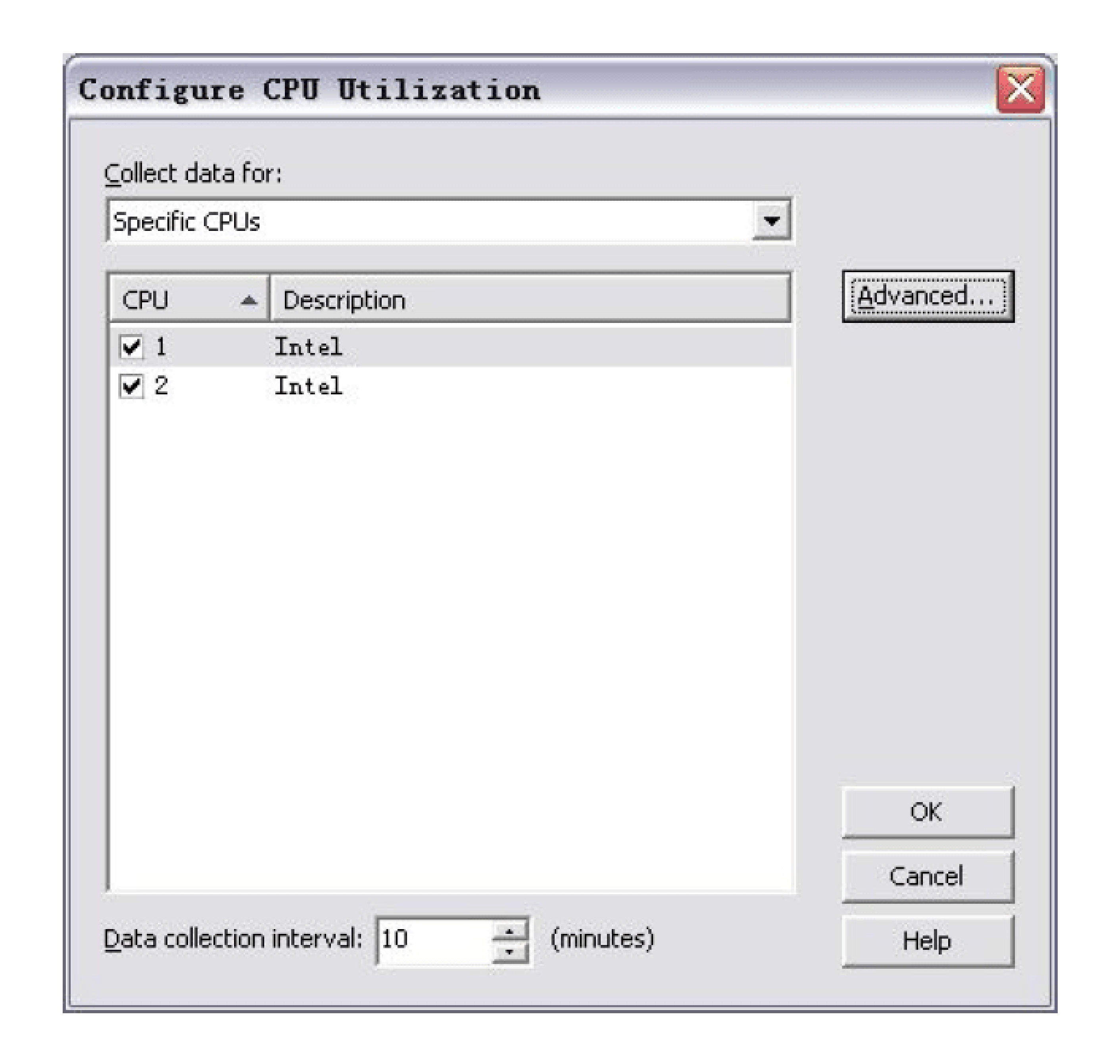


图 7-2 查看 CPU 硬件信息

选择 Interface Utilization 可查看其接口状态信息，包括虚拟机接口，如图 7-3 所示。

7.1.2 无法采集 Windows 信息故障分析

有的情况通过 WhatsUp 采集 Windows 主机信息不成功，会弹出提示信息，提示采集对象中未提供 SNMP 代理服务、对方对信息采集无应答或者网络存在故障，如图 7-4 所示。

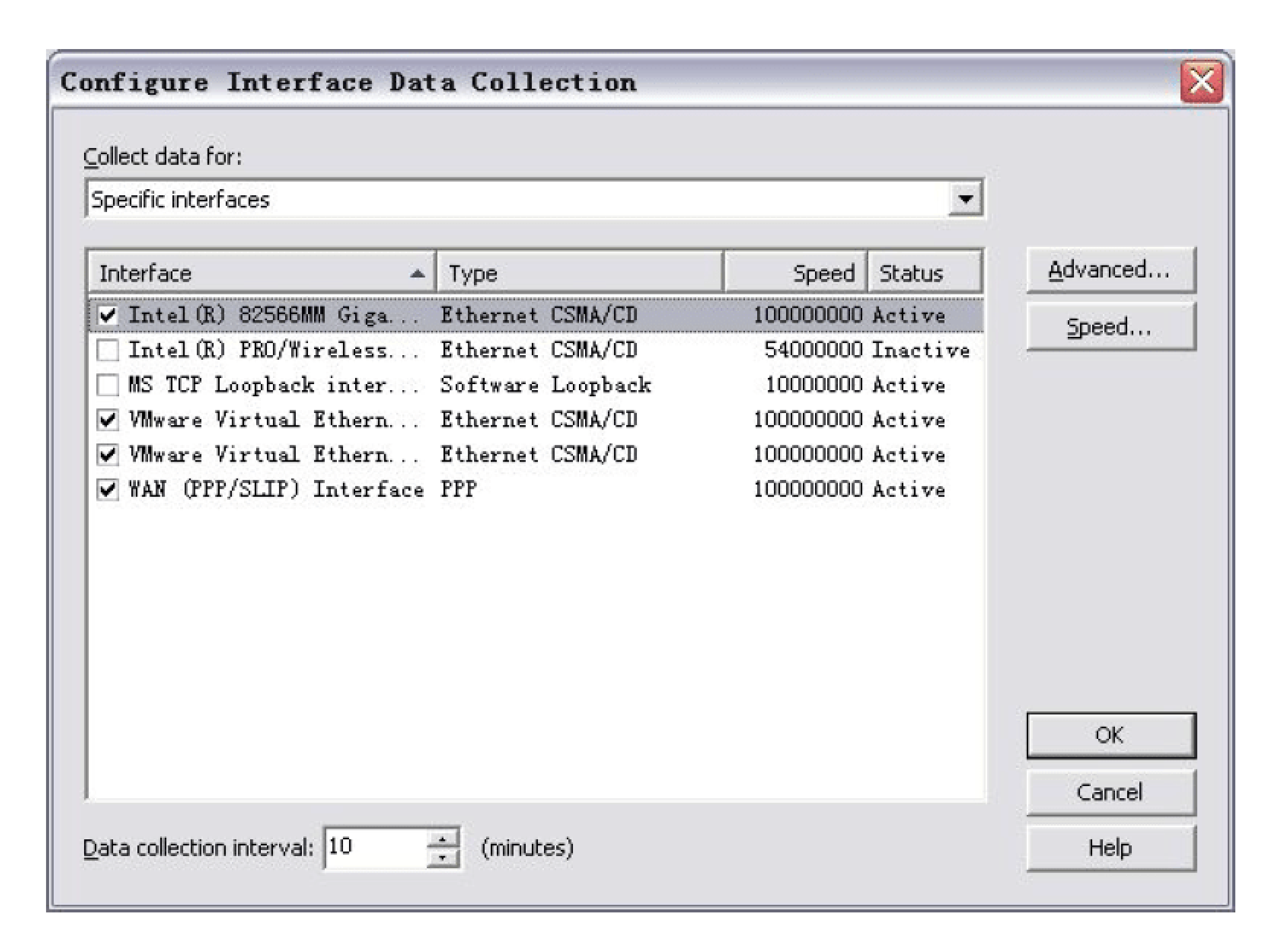


图 7-3　查看接口信息



图 7-4　无法采集 Windows 主机信息

可能导致无法采集到 Windows 设备信息的原因如下：

- 被采集 Windows 系统设备中未安装 SNMP 服务组件，或未设置 SNMP 字符串。
- 访问设备的凭证与设备中的社区字符串不匹配。
- Windows 主机 SNMP 服务未启动，该情况出现的较多，SNMP Service 可能因为安装了其他第三方 SNMP 代理程序而停止服务，或由于系统异常而导致服务停止，所以首先需要保证设备的 SNMP 服务处于正常启动状态。
- 由于防火墙的原因导致无法通过 SNMP 获取对方设备的信息。

7.1.3　Linux 系统主机信息采集

在对 Linux 服务器做了 SNMP 配置之后，就可以通过 WhatsUp Gold 采集其硬件信息了，操作步骤与采集 Windows 主机硬件信息一样。如下：

在主界面设备列表中，选择一台开启 SNMP 服务的 Redhat Linux 系统设备，打开该设备的属性界面，并添加 Credentials 页面中的 SNMP 访问凭证。

选择该设备的 Performance Monitor 选项页，选择要查看的选项后就能实现信息采集，

选择 CPU Utilization 查看 Linux 主机的 CPU 信息，如图 7-5 所示。



图 7-5　Linux 主机 CPU 信息

此处列出了 Linux 主机 4 行 CPU 信息，但并非表示该主机有 4 个 CPU，而是该主机 CPU 是四核的 AMD CPU。

查看磁盘信息，选择 Disk Utilization 选项查看磁盘分区及容量等信息，如图 7-6 所示。

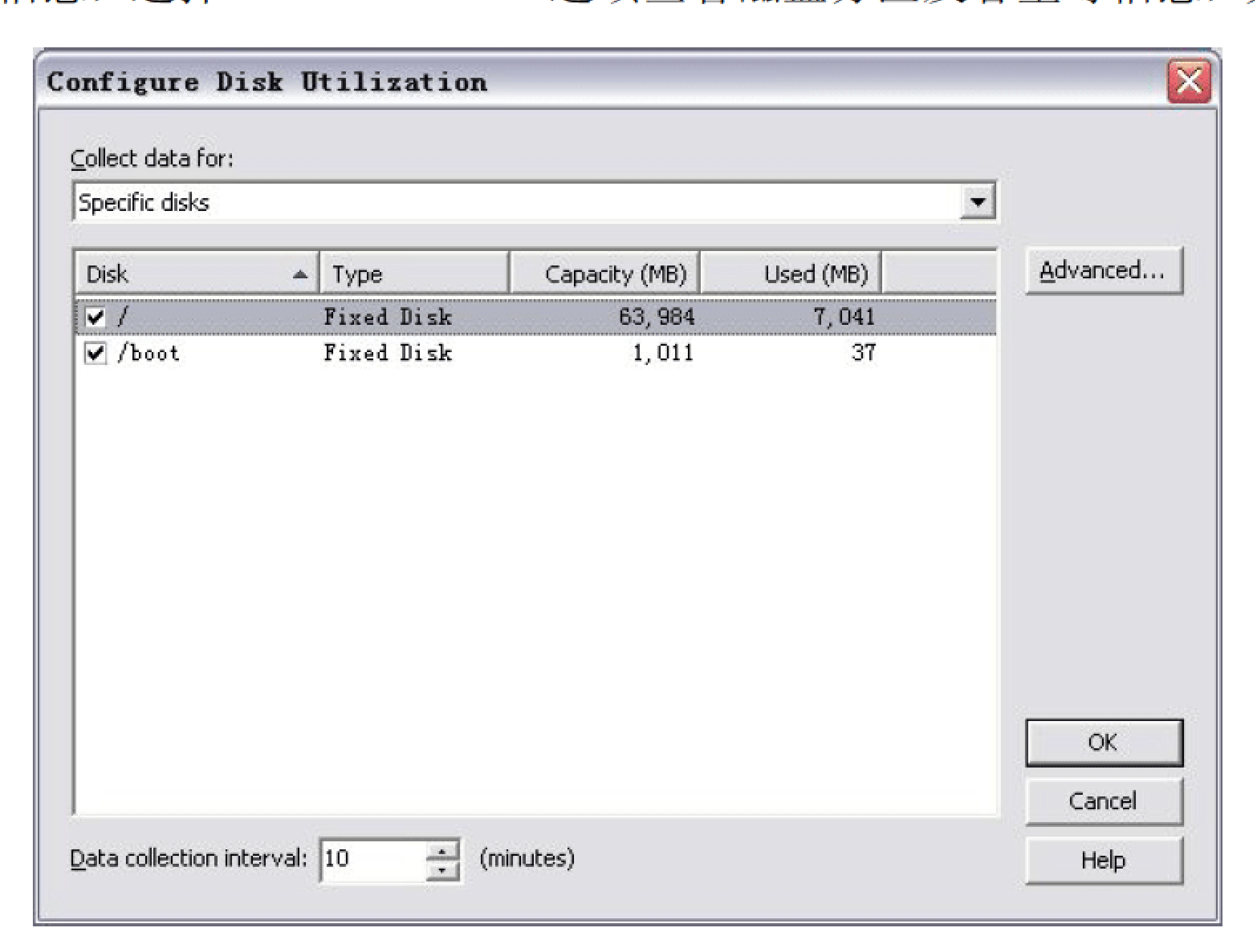


图 7-6　Linux 主机磁盘信息

在 Linux 系统下最少需要两个分区，该 Linux 主机包含两个磁盘分区，如下：

- / 主分区，也叫根分区，是 Linux 文件系统的基础，是所有文件的顶级根。

- /boot 分区，它包含了操作系统的内核和在启动系统过程中所要用到的文件，有了单独的/boot 启动分区，即使主要的根分区出现了问题，计算机依然能够启动。

Linux 主机的磁盘分区与 Windows 主机有所不同，此处将 Windows 和 Linux 系统的磁盘分区做简单介绍。在 Windows 系统中只包含一个主分区，并在扩展分区上增加逻辑分区，最后创建了几个分区就有几个驱动器，通过选择每个分区的字母标识来管理分区上的文件和目录。

而在 Linux 中规定，硬盘的分区主要分为 Primary Partion（基本分区）和 Extension partion（扩充分区）两种，基本和扩充分区的数目之和不能大于 4 个。基本分区（也称为主分区）可以马上被使用但不能再分区，扩充分区必须再进行分区后才能使用，也就是作为逻辑分区使用。

选择 Memory Utilization，可查看该 Linux 主机内存信息，如图 7-7 所示。

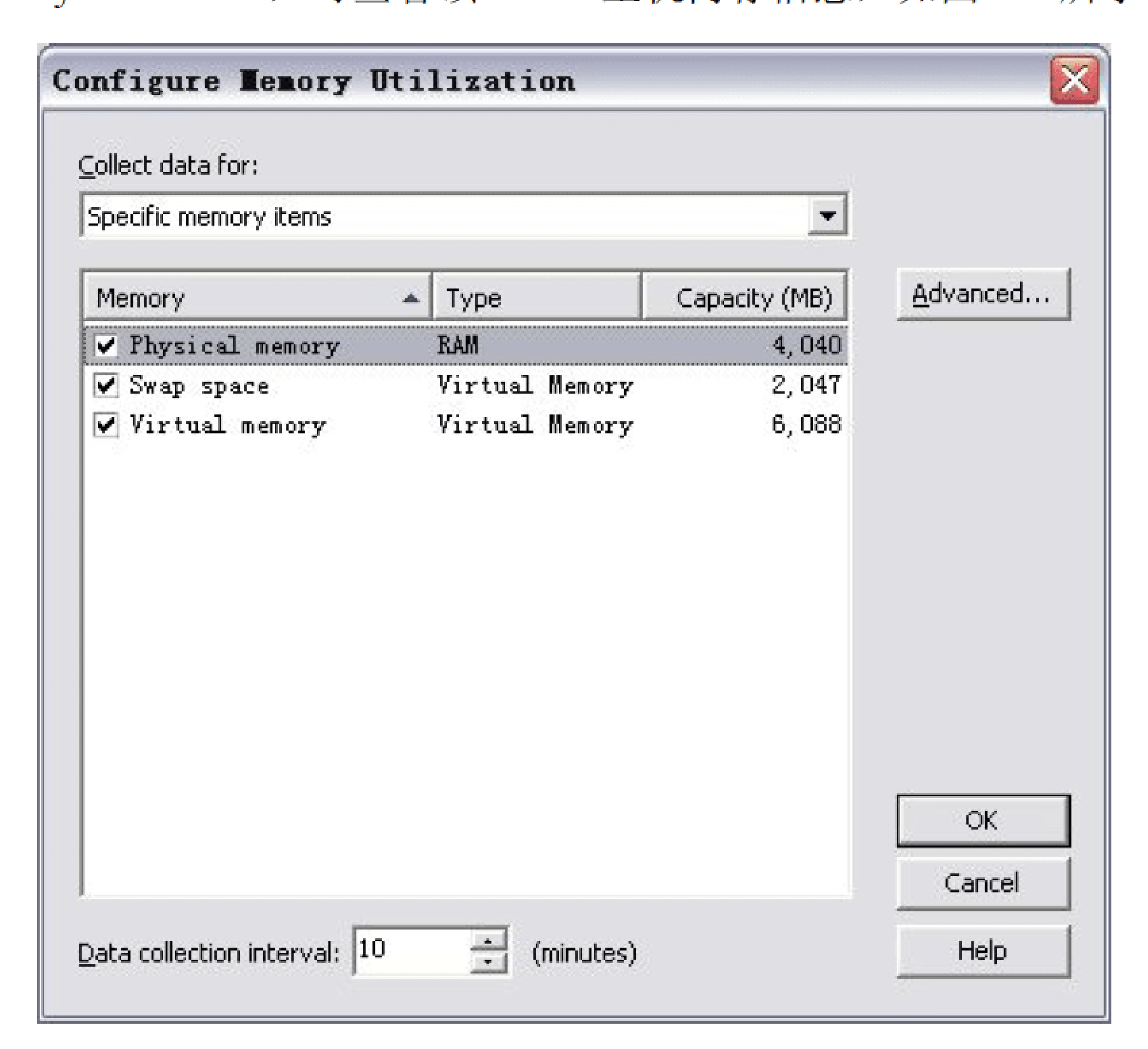


图 7-7　Linux 主机内存信息

在该 Linux 设备中，分别列出了 Linux 主机的物理内存和虚拟内存大小和 Swap Space 的大小。Linux 系统支持 Virtual Memory（虚拟内存），虚拟内存作为物理内存 RAM 的扩展。Swap Space 则是硬盘中用作虚拟内存的部分，作为数据的交换空间。

7.1.4　网络设备信息采集

1．采集路由器接口信息

配置路由器开启 SNMP 代理服务后，在 WhatsUp Gold 路由器设备属性中配置访问

SNMP 凭证后，选择查看该路由器的 Interface Utilization 选项，即可看到该路由器所有接口信息，包括激活的端口和未启用的端口信息。该路由器包含千兆光口以及若干电口，如图 7-8 所示。

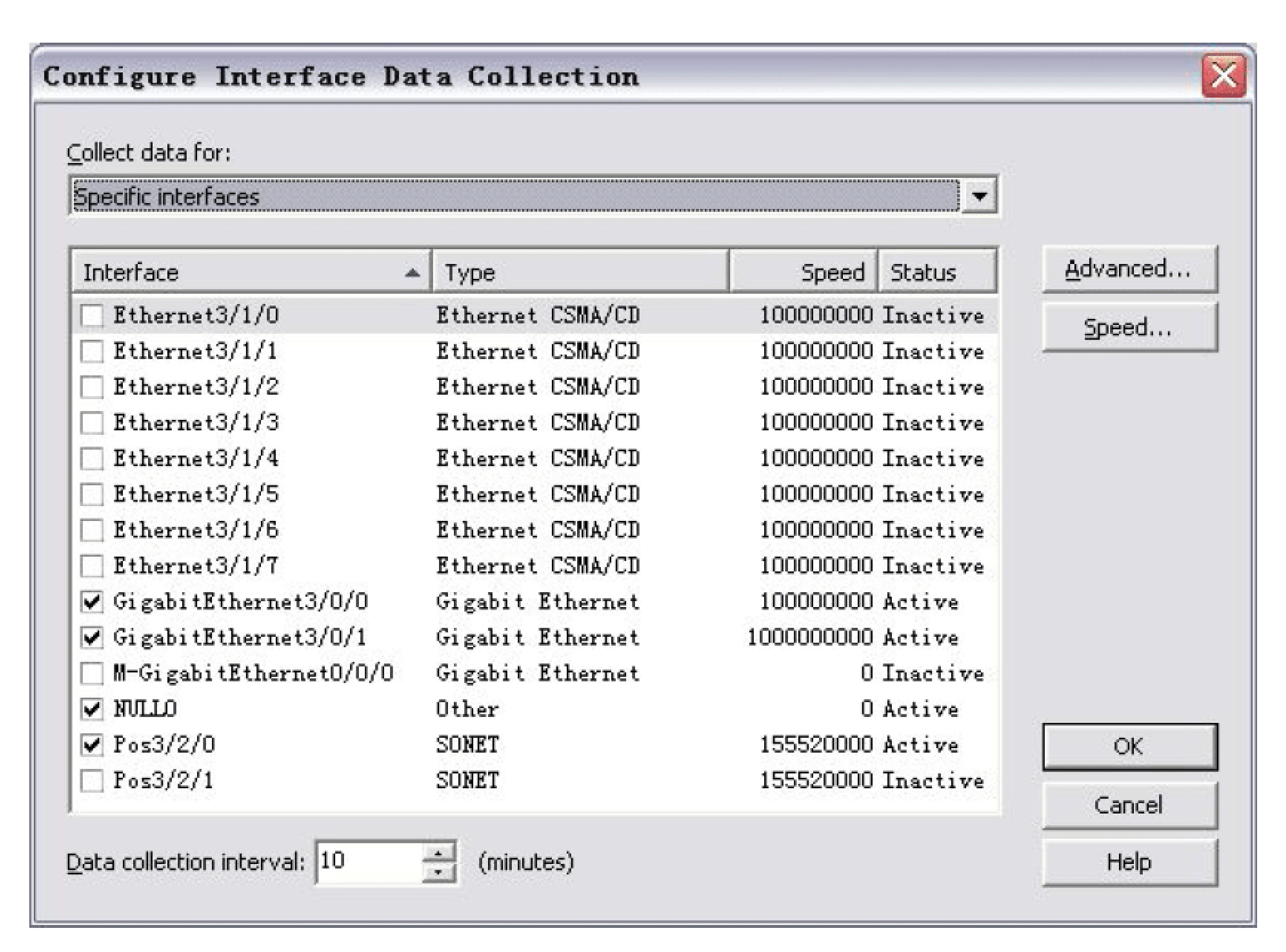


图 7-8　查看路由器的接口信息

如果需要采集路由器 CPU 信息，则可能因 WhatsUp Gold 缺乏该路由器 MIB 库文件或者路由器并无 CPU 而导致无法采集到 CPU 信息，此时将弹出错误提示，如图 7-9 所示。

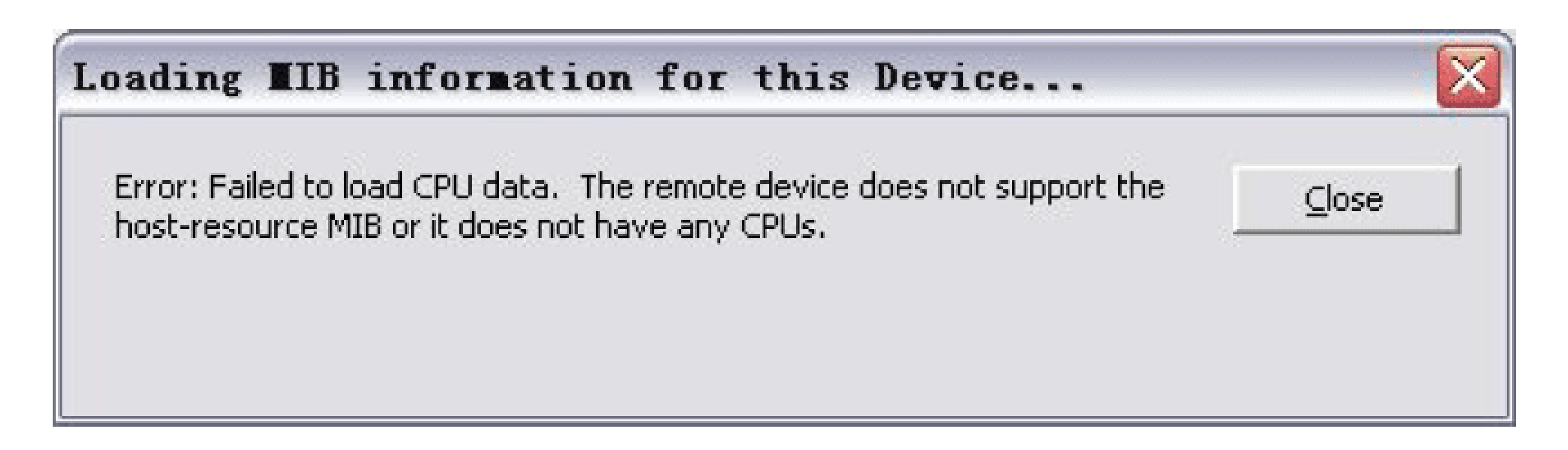


图 7-9　无法采集到路由器 CPU 信息提示

2．采集交换机信息

对于交换机设备，最为关注的就是交换机的接口状态。在配置交换机开启 SNMP 服务后，在 WhatsUp Gold 设备列表中，同样在性能监测页面选择 Interface Utilization 选项，即可通过 SNMP 采集到交换机接口信息，如图 7-10 所示。

同样，如果在性能监测界面能够采集到交换机的这些端口信息，那么在该交换机的 Active Monitors（主动监测）页面，也能够自动发现这些端口，并对各端口实行轮询监测，如图 7-11 所示。

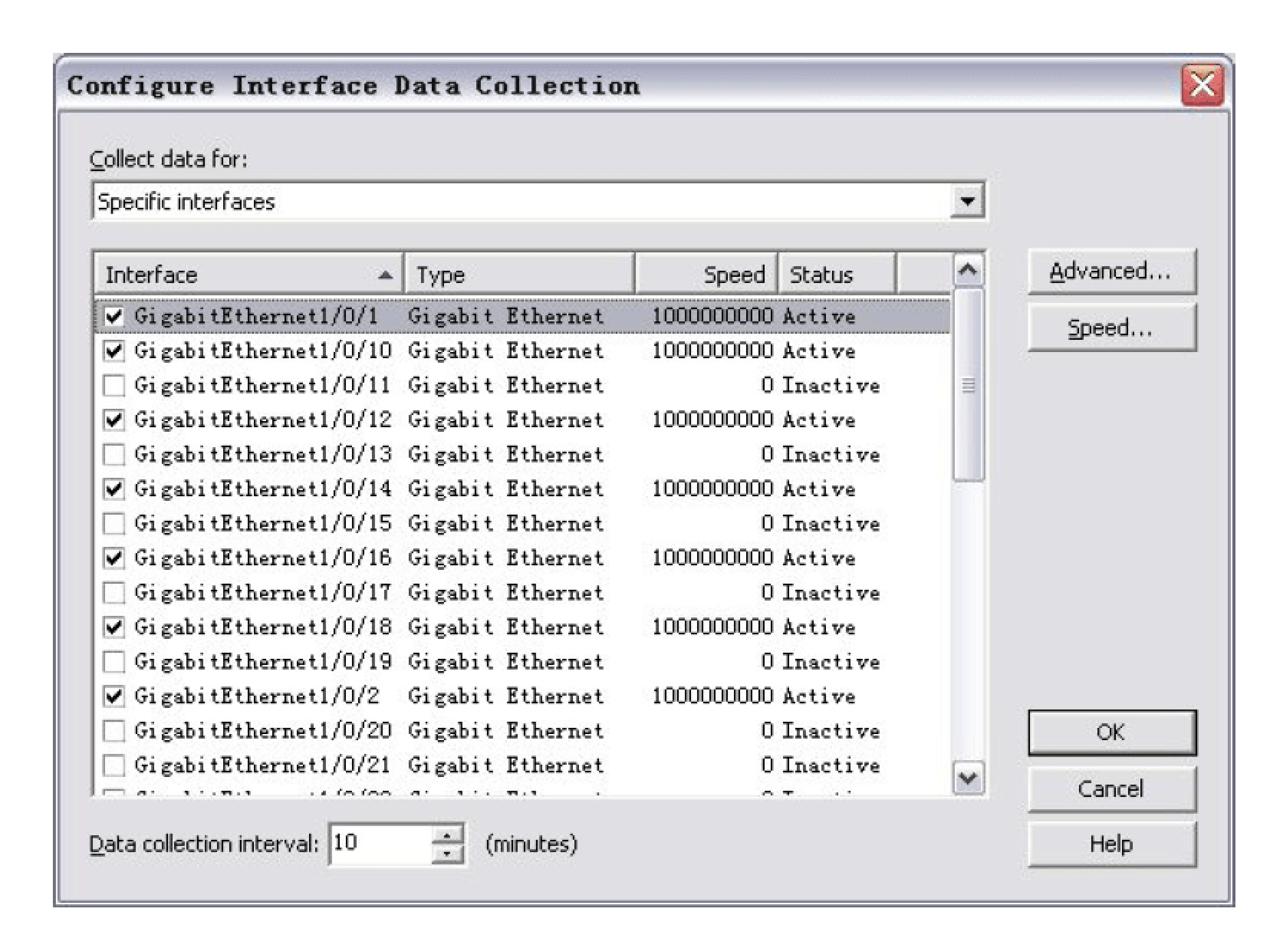


图 7-10　采集交换机接口信息

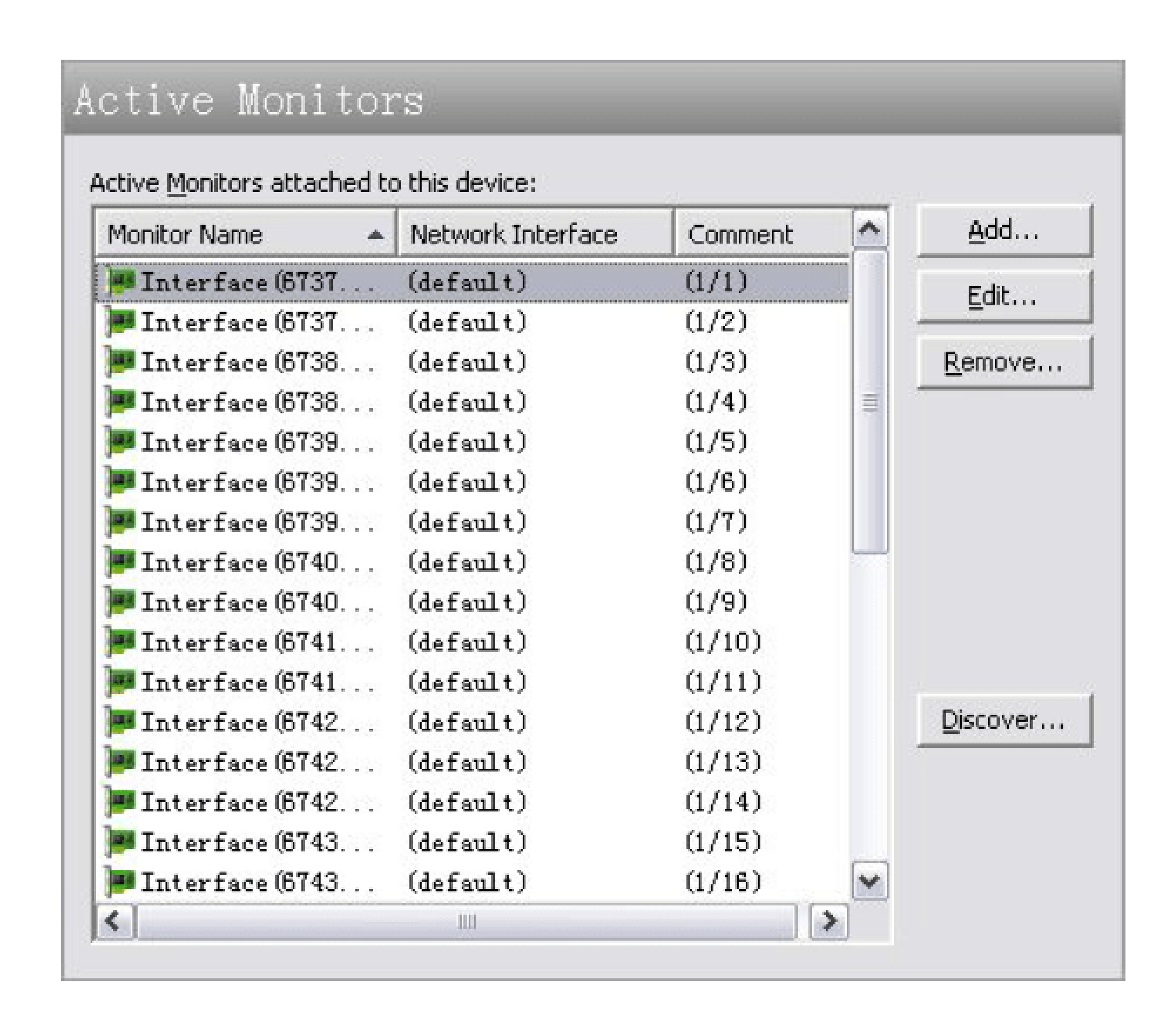


图 7-11　交换机的主动监测对象

7.2 Performance Monitors 性能监测

除了通过 WhatsUp Gold 自带的 Performance Monitors 监测项目获取系统基本信息外，还可根据需要添加自定义的性能监测对象，实现对系统和设备性能更深入地监测，包括实现对特种设备的监测。以下介绍通过 SNMP 方式和 WMI 方式实现对特殊设备的性能监测。

在介绍特殊设备前，首先需要获取特殊设备的 MIB 文件以及将 MIB 文件导入到 WhatsUp Gold 中，

7.2.1 在 WhatsUp Gold 中添加 MIB 文件

如果要添加一些特殊设备的 MIB 文件到 WhatsUp Gold 系统中，可通过联系设备制造商或者查找其官方网站等方式，获取设备的 MIB 文件和使用指南。

要导入 MIB 文件到程序中，只需复制文件到 WhatsUp Gold 安装目录下的 Mibs 文件夹中，路径为...\WhatsUp\Data\Mibs，复制结束后，重新开启 WhatsUp Gold 程序即完成导入。通过 MIB 浏览窗口可查看导入的 MIB 文件。

注意：如果在网页模式下使用 WhatsUp Gold，在添加 MIB 文件后，需要重启网页服务。

有的时候，设备官方网站下载的 MIB 文件复制到 Mibs 目录下无法启用，还需要使用 WhatsUp Gold 自带的 MIB 编译工具 Mibextra.exe 进行编译才能正常使用。该工具使用步骤如下：

（1）将下载的文件解压至一个简单路径的目录下，例如将力博特精密空调设备的 MIB 文件解压至 C:\libert\目录下。如果路径中包含了空格字符（如 C:\Program Files\），在使用 Mibextra 编译时会出错，所以尽量将 MIB 解压到简单路径目录中。

（2）使用 Mibextra 工具进行编译。打开【开始】菜单中的【运行】命令，并单击【浏览】按钮，在浏览对话框中选择 WhatsUp Gold 安装目录中的 Mibextra.exe 工具，如图 7-12 所示。

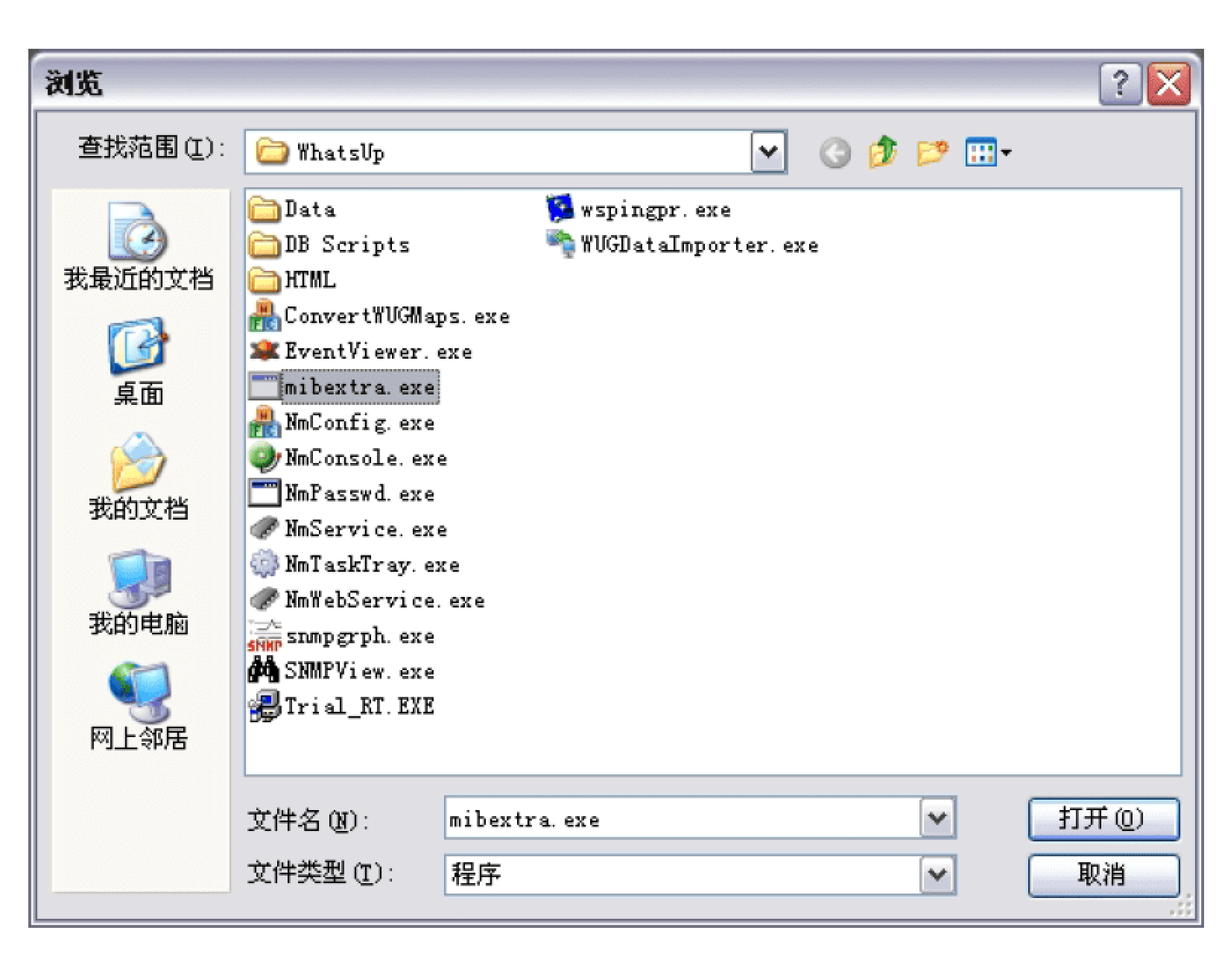


图 7-12　打开 Mibextra 编译工具

（3）选择该工具后，其目录将被添加到【运行】中，然后在该目录语句后面加入要编译的 MIB 文件目录，并加上“*”字符（如 C:\libert*），单击【确定】按钮即对该目录下

所有的 MIB 文件进行编译，如图 7-13 所示。



图 7-13 编译 MIB 文件

如果编译过程中报错，那么有可能是 MIB 文件不完整。如果 MIB 文件之间存在关联性和依赖性，那则需要将关联的文件也放入同一文件夹进行编译。

（4）编译正常结束后，再将解压目录下的所有 MIB 文件复制至...\WhatsUp\Data\Mibs 目录下，重启 WhatsUp Gold 程序，即完成了编译和导入 MIB 文件的操作。

性能监测项目，能够监测和采集大多数的网络设备的日常性能，但如果需要监测设备的特殊性能参数，则需要建立针对特殊设备的自定义性能监测项目。

7.2.2 SNMP 方式监测机房温度

对于设备的日常运行环境，保持机房温度恒定是非常重要的。温度过低或者过高，都可能会导致设备死机或造成硬件损害。机房专用空调能够保持机房温度为 25℃，但随着机房设备的不断增加，机房增加了额外的热源，就有必要实时了解机房温度以确保冷却效果。

以力博特（Liebert）空调为例，介绍实现对机房温度的监测。操作步骤如下：

（1）首先要求力博特空调设备安装了远程监控接口板，该接口板能够采集空调设备运行情况并可进行读取。在开启了接口板 SNMP 功能，设置接口板 SNMP 参数和 IP 地址后，可远程读取空调的运行参数，包括温湿度、告警信息、运行方式等。

（2）使用 WhatsUp Gold 对空调设备进行监测，还需下载该空调设备的 MIB 文件并导入...\WhatsUp\Data\Mibs 文件夹中。获取 MIB 文件，可访问力博特空调的官方网站 http://www.emersonnetworkpower.com/en-US/Brands/Liebert/Pages/default.aspx，该网站提供了支持各类操作系统的 MIB 文件下载，文件的后缀名为.MIB，下载后的力博特全系列设备 MIB 文件如图 7-14 所示。

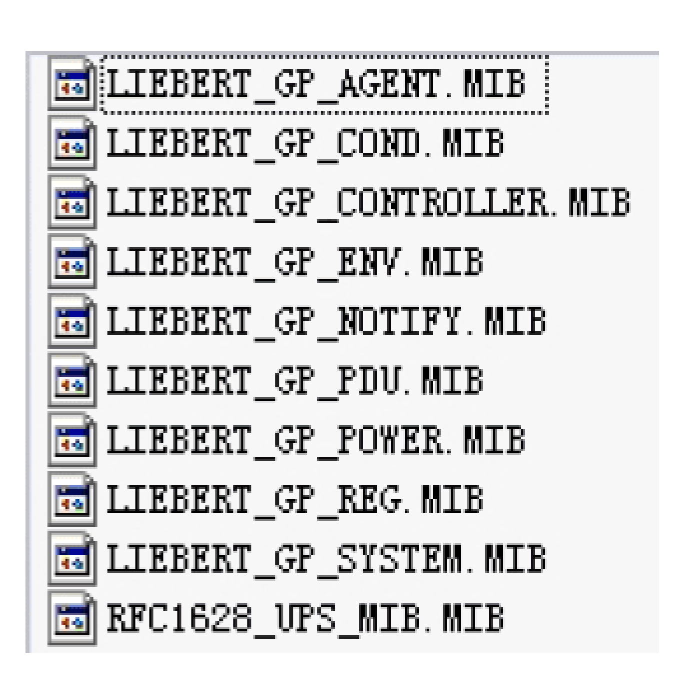


图 7-14 力博特系列设备 MIB 文件

注意：如果采用支持 SNMP 协议的温度传感器来获取空调温度，同样需要将该型号温度传感器的 MIB 文件复制至\WhatsUp\Data\Mibs 文件夹中，然后通过 WhatsUp Gold 监测和跟踪传感器的 IP 地址，实现对温度的实时掌握。

（3）在 WhatsUp Gold 主界面设备列表视图或拓扑视图中，打开快捷菜单并选择 New Device 菜单，打开添加设备对话框，并输入空调远程监控接口板的 IP 地址，如图 7-15 所示。



图 7-15　添加温度传感器设备

在该界面中，还需要进行其他配置。单击 Advanced（高级选项）按钮，在弹出的对话框中清除主动监测和性能计数器监测窗的复选框，仅保留 Ping 的主动监测 Ping active monitor，同时选中 Identify device via SNMP 和 Resolve host name 复选框，即允许识别设备的 SNMP 通用接口和解析主机名，然后在 SNMP read communities 文本框中输入访问认证字符串，此例中为默认值 public，如图 7-16 所示。

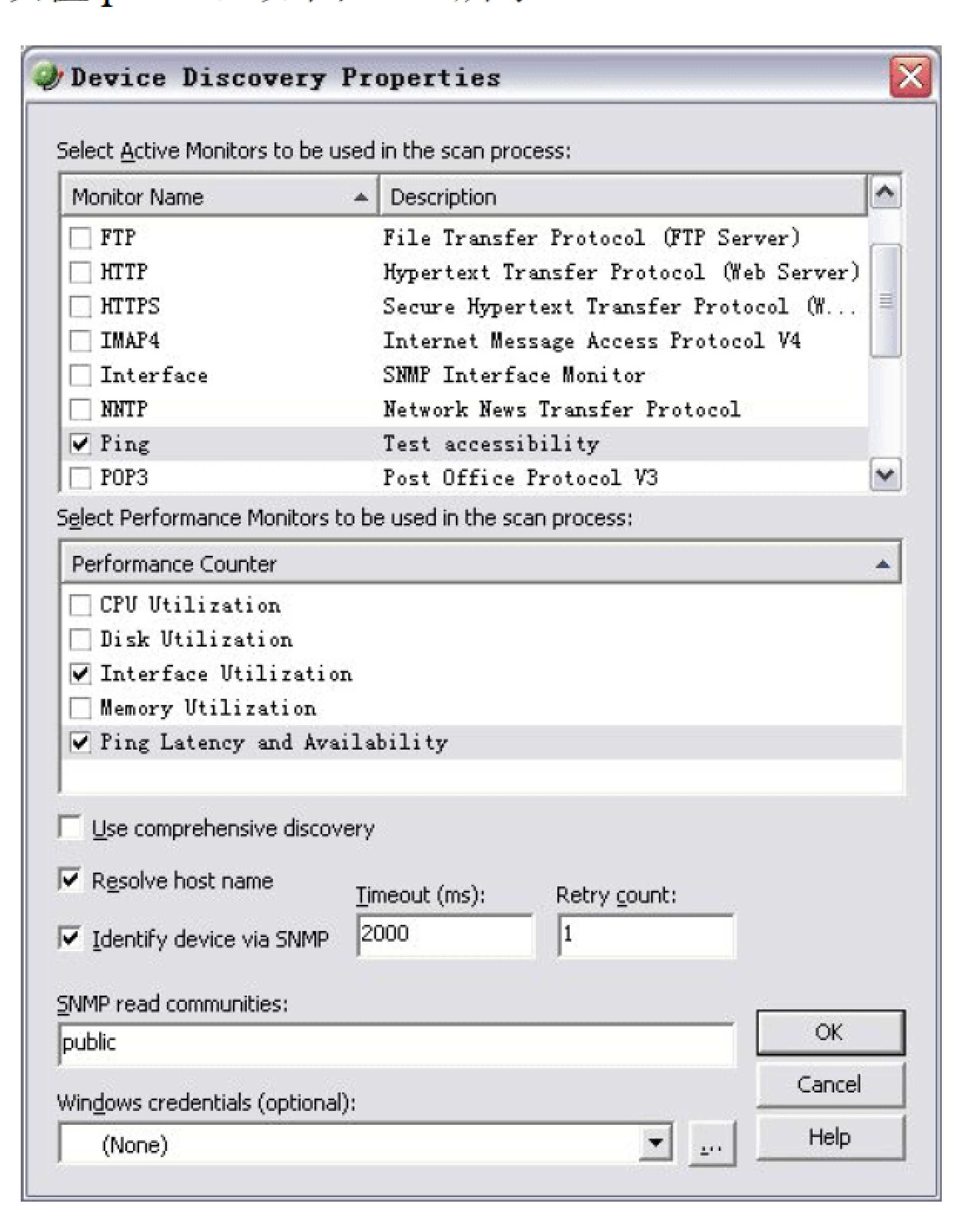


图 7-16　配置设备查找属性

（4）设置完高级选项后，返回添加设备窗口并选择下一步查找设备。检测出该设备后，将直接弹出设备属性 Device Properties 窗口，选择 Performance Monitors 页面，并在界面下方添加自定义监测项目部分，单击 New 按钮，在新建监测项目类型界面的下拉框中选择 SNMP Performance Monitor 选项，如图 7-17 所示。

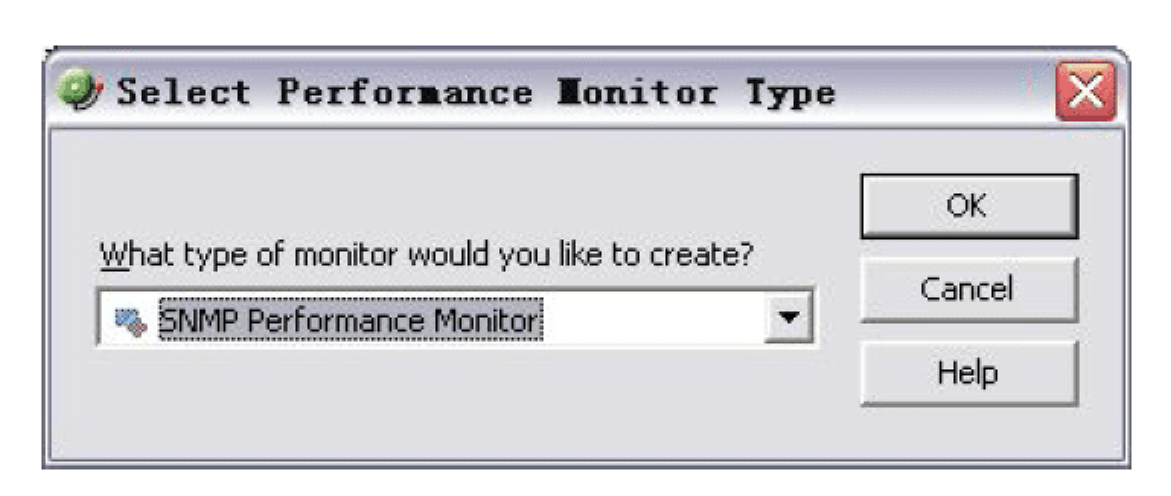


图 7-17　选择性能监测项目类型

（5）单击 OK 按钮进入下一步，在弹出的 Add SNMP Performance Counter 窗口中（如图 7-18 所示），在 Name 文本框中输入名称为 Temperature Monitor，在 Performance Counter 文本框中需要添加的是接口板的对象标识（OID），在 Instance 文本框中需要添加接口板中用于采集温度的实例节点。该两项数值可通过单击文本框右侧的【...】浏览按钮进行添加。在 Collection Interval（min）文本框中输入 10，让 WhatsUp Gold 每 10 分钟收集一次温度数据。

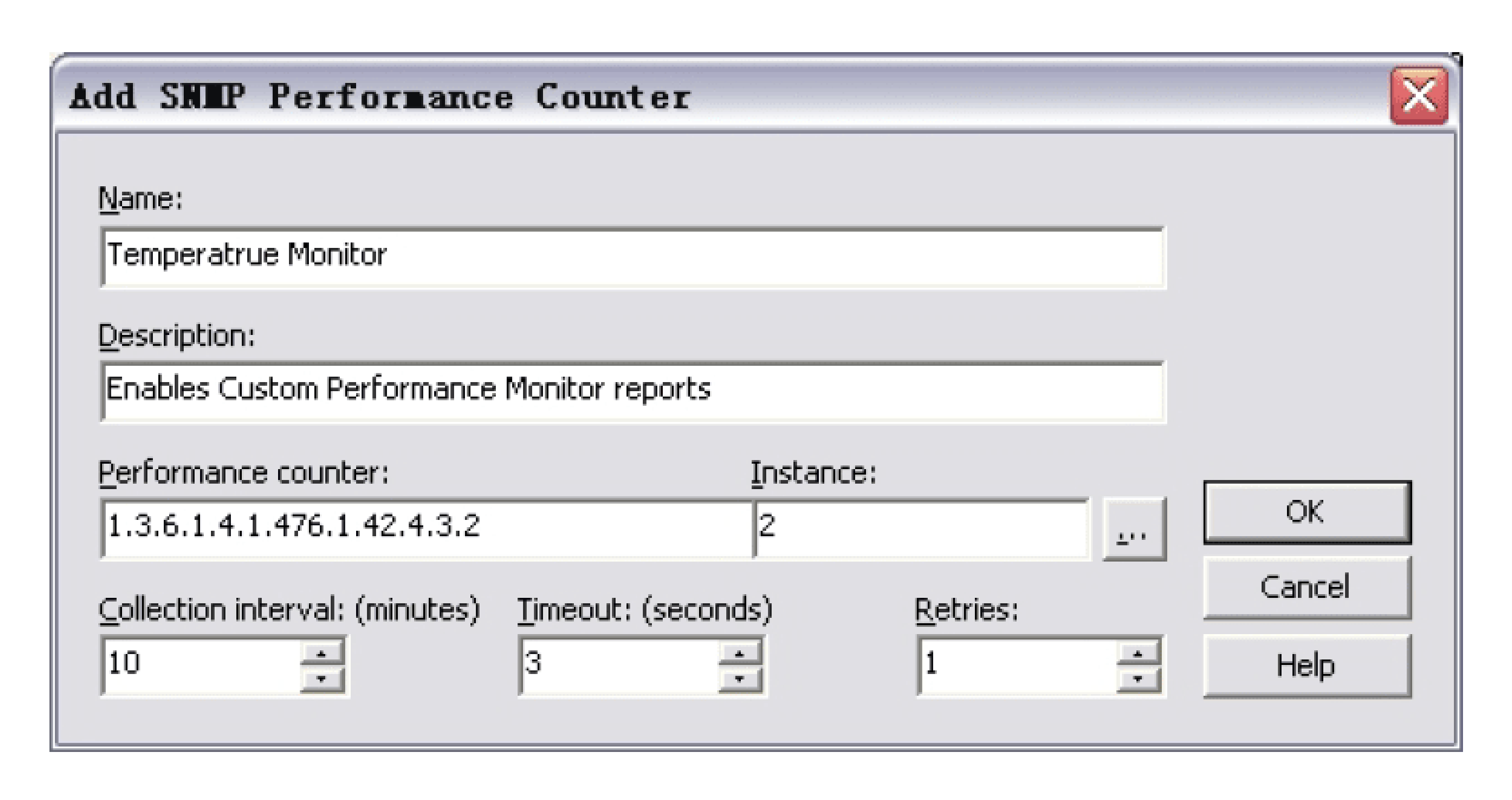


图 7-18　配置 SNMP 方式性能监测项目

此处详细介绍对象标识的获取。单击【...】按钮打开 SNMP MIB Walker 窗口，其中列出了空调设备的 MIB 库，在 MIB 树中找到采集温度值的对象（一般在 private\enterprises 目录下）。选择空调监测节点 lgpAcProducts 后，界面下方的 Object ID 文本框中会自动显示该节点对象的 OID 值（如图 7-19 所示），然后选择代表温度值的 Instance 参数（Instance 参数的描述，可参考 Liebert 设备 SNMP 管理手册）。

（6）配置完成后，返回设备属性的 Performance Monitor 页面，可以看到已经为空调设备添加了采集温度数值的性能监测项目。在添加后 WhatsUp Gold 开始收集数据，经过几次轮询数据采集后，将能采集到足够的数据来生成报表。

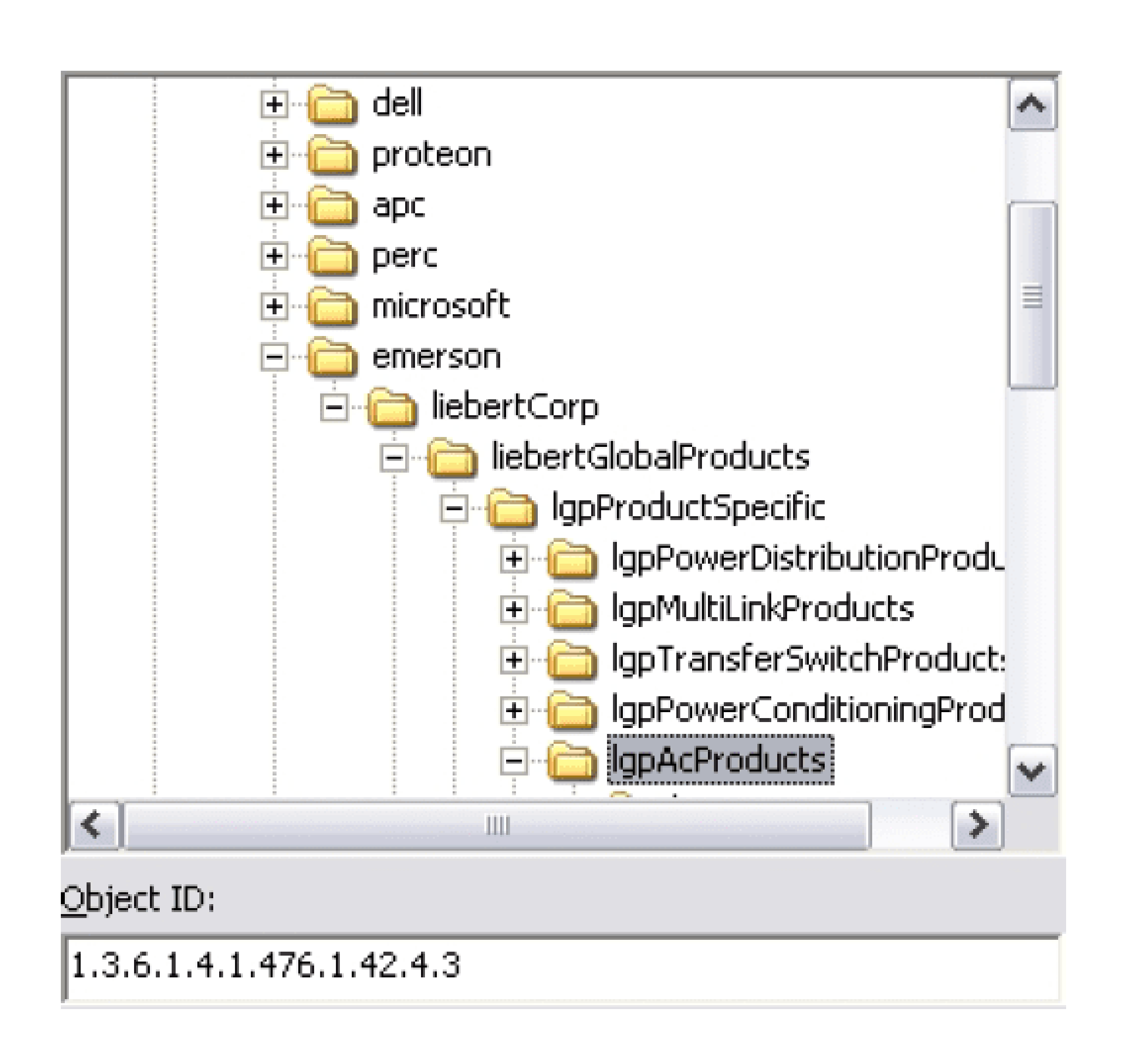


图 7-19　选择温度传感器 OID

（7）查看采集到的温度信息报表。在 Device 视图或 Map 视图中，打开该空调设备快捷菜单，选择 Device Reports 菜单命令，打开该设备的报表界面，如图 7-20 所示。

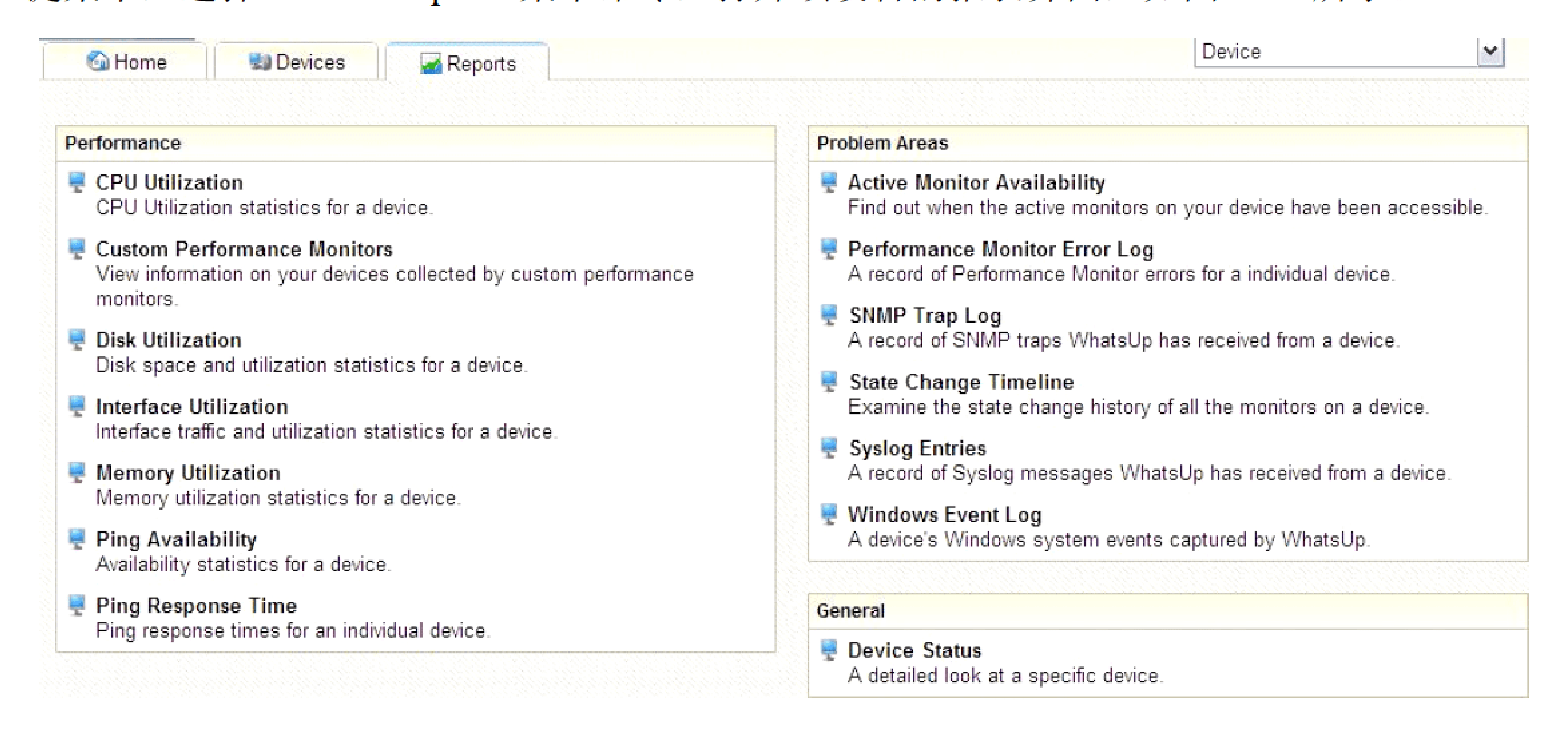


图 7-20　设备信息报表

（8）选择 Custom Performance Monitors，该项报表为自定义性能监测对象的数据，包括了自从设备被添加后所收集到的所有数据。此处查看该空调设备温度值图表，如图 7-21 所示。

7.2.3　SNMP 方式监测 UPS 状态

要对 UPS 设备的电压、状态和电池等信息进行监测，那么首先需要 UPS 主机中安装了远程监控接口板或者安装了支持 SNMP 协议的 UPS 传感器，并对设备设置 IP 地址、打开允许 SNMP 管理和设置 SNMP 社区字符串，即可通过 WhatsUp Gold 实现对 UPS 性能的

实时监测。

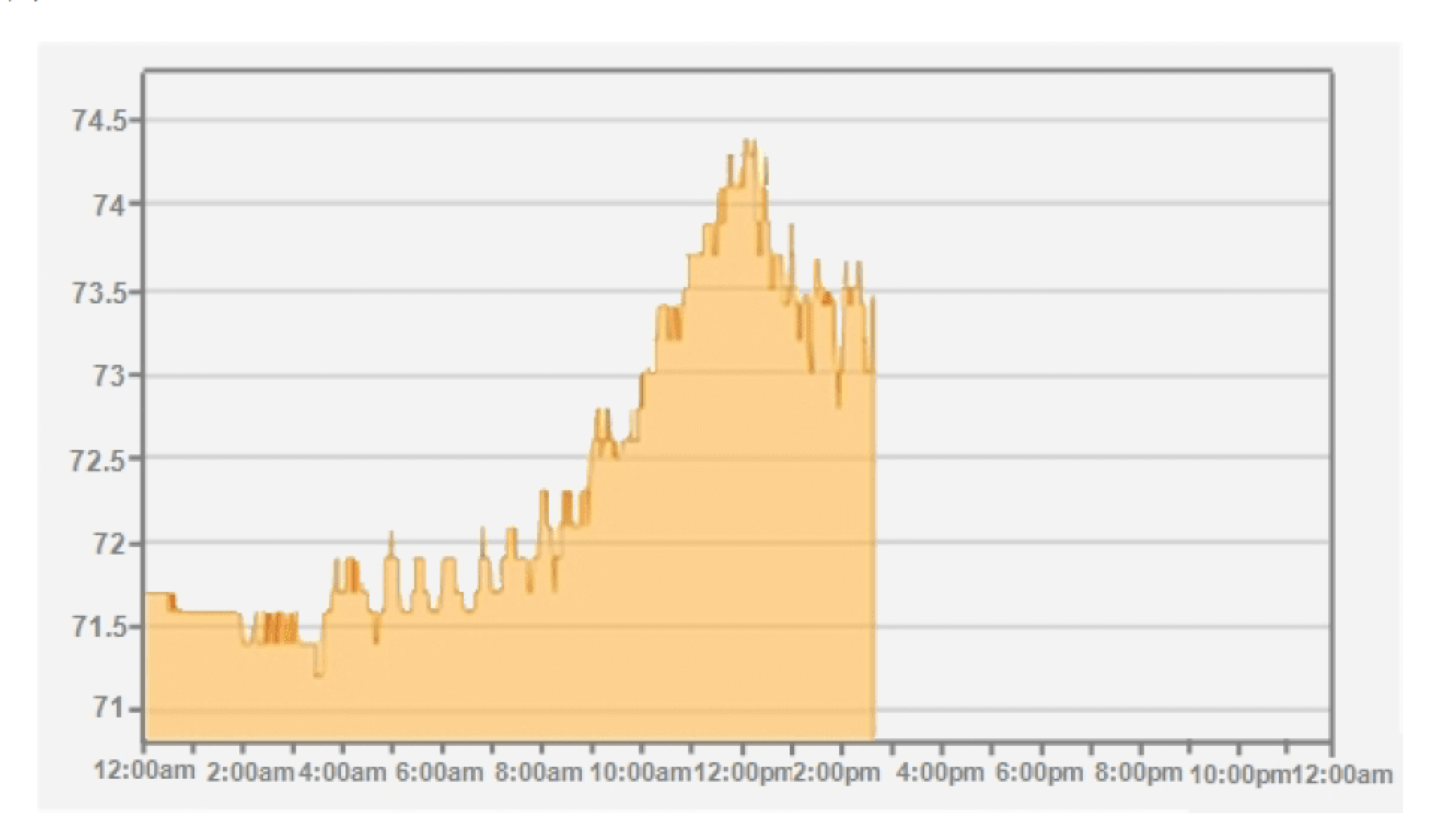


图 7-21　查看温度取值报表

此处以 APC 的 UPS 主机为例进行介绍。APC 的 UPS 主机远程监控设备如图 7-22 所示。



图 7-22　力博特 UPS 传感器和远程监控接口板

本例以远程监控接口板方式做介绍。配置步骤如下：

（1）通过 WhatsUp Gold 监测 UPS 主机性能，首先需要将 UPS 主机厂家提供的 MIB 文件复制到...\WhatsUp\Data\Mibs 目录中，这些以.mib 为后缀的 MIB 文件，可通过 APC 的官方网站进行获取，复制到 Mibs 文件夹之后，UPS 主机的 MIB 文件如图 7-23 所示。



图 7-23　UPS 主机的 MIB 文件

（2）在 WhatsUp Gold 主界面中，通过 UPS 接口板的 IP 地址查找和添加该设备后，选择该设备属性界面的 Performance Monitors 页面，为该 UPS 主机添加自定义的性能监测项目。选择 New 并在新建对话框中输入名称及描述信息，如图 7-24 所示。

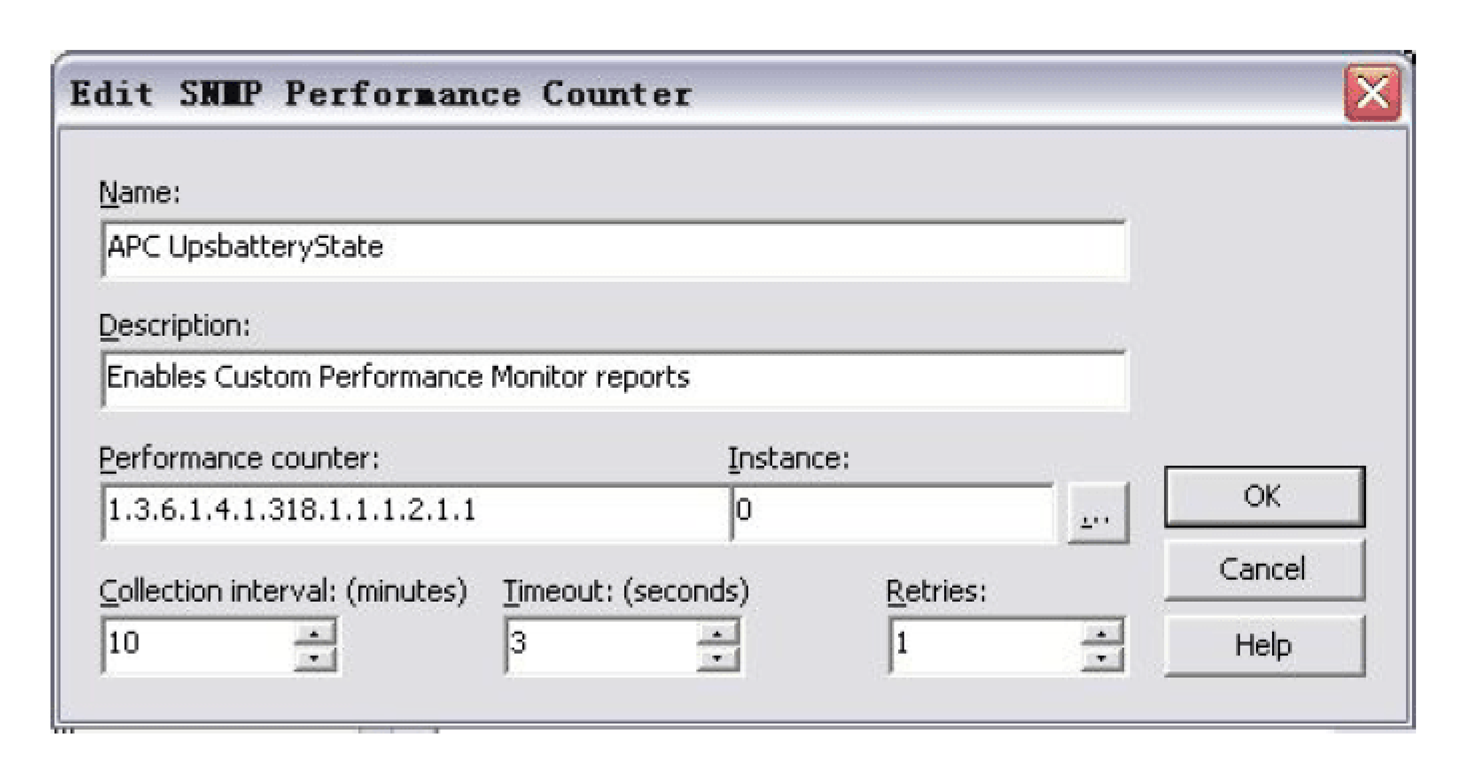


图 7-24　添加自定义的性能监测项目

（3）单击 Instance 右侧的【...】按钮，打开 MIB 实例选择界面。同样，APC UPS 设备的 MIB 文件被安装在 Private | enterprises 目录下，如图 7-25 所示。

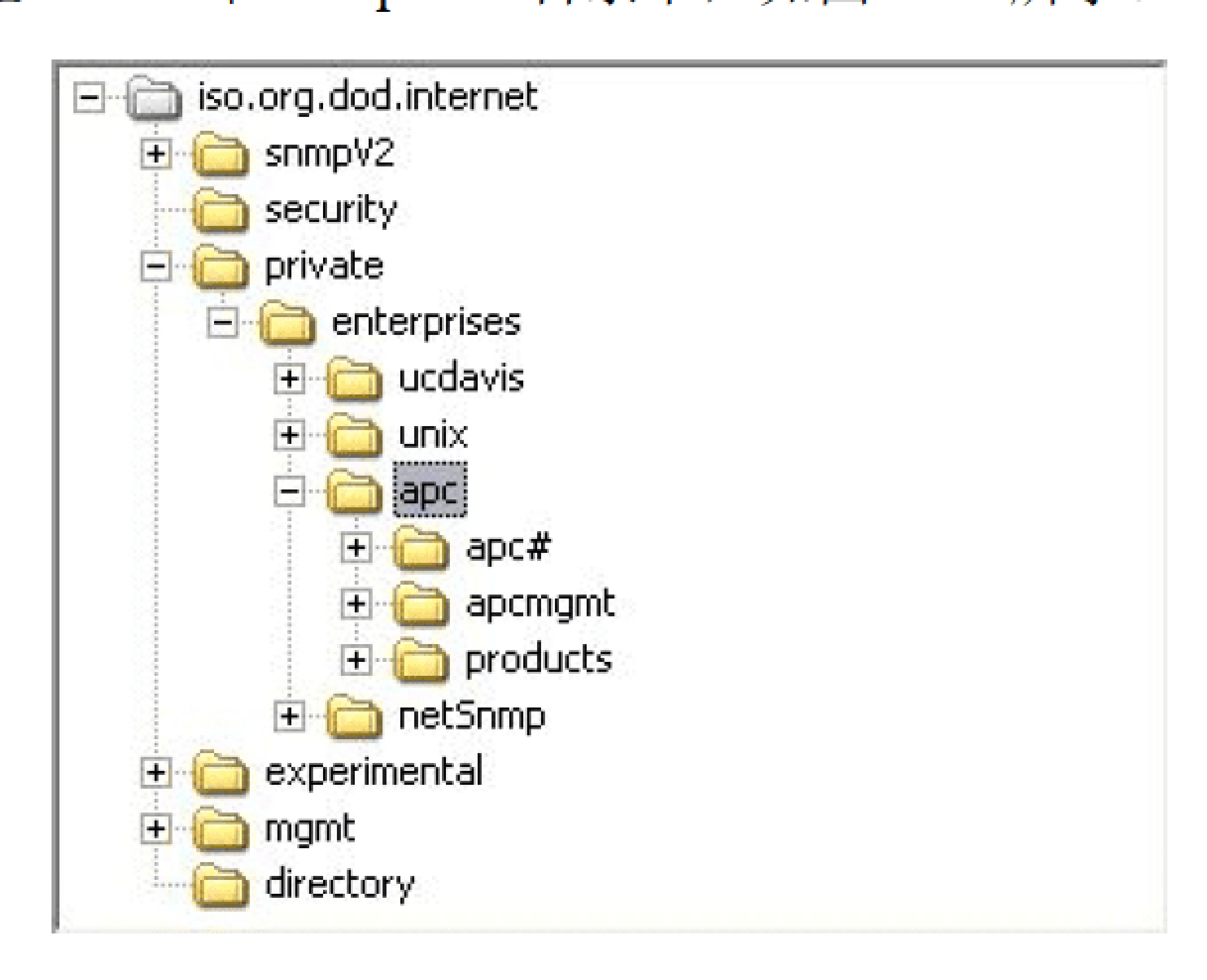


图 7-25　APC UPS 的 MIB 节点

（4）选择 APC 的监测对象，此处选择目录树中 products | har | dware | ups | upsBattery 目录下的 upsBasicBatteryStatus 实例，实现对电池运行状态的监测，如图 7-26 所示。

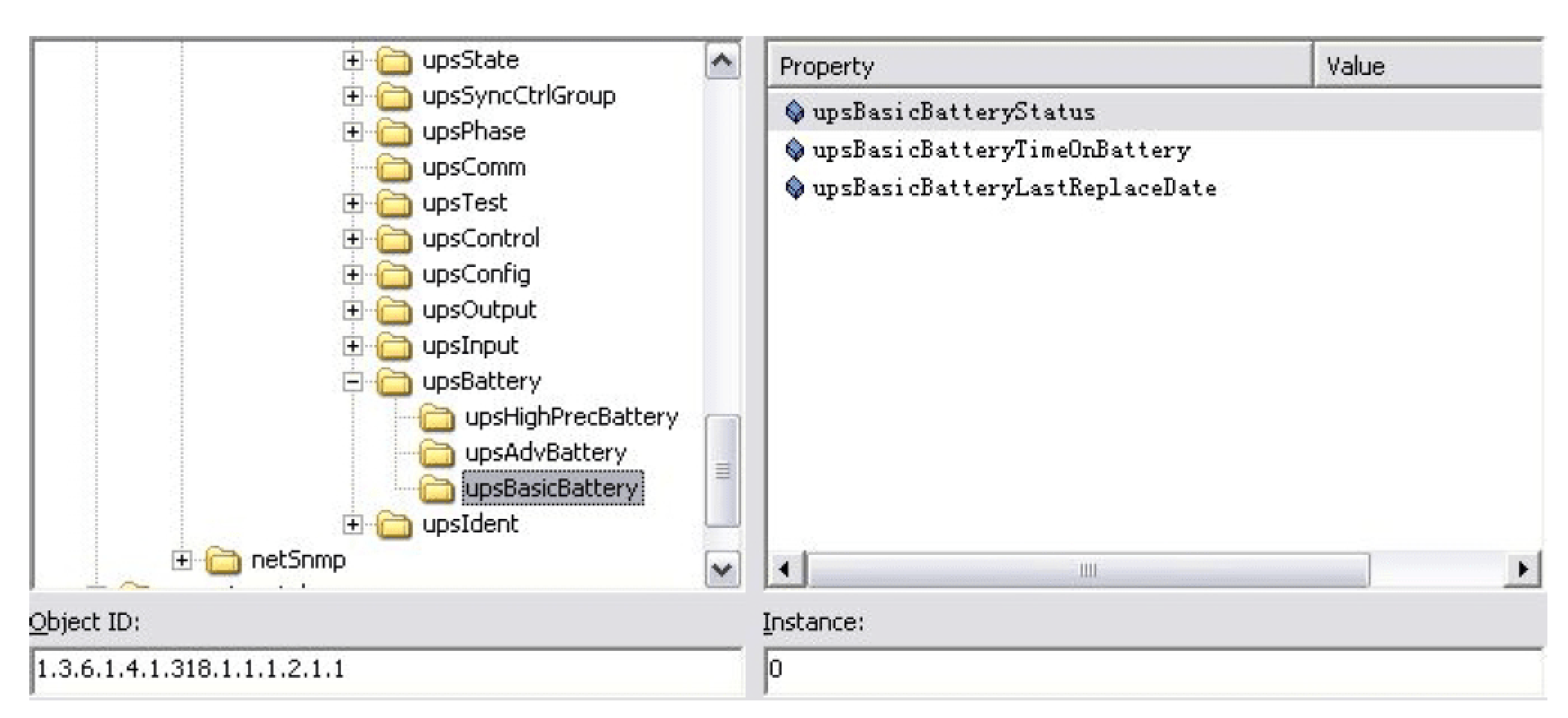


图 7-26　APC UPS 的 MIB 节点实例

（5）添加完成之后，可以在性能监测界面看到刚刚建立的 UPS 电池状态监测项目，WhatsUp Gold 将对该监测内容进行轮询操作，如图 7-27 所示。

（6）在完成设置之后，可登录到 Web 模式中，查看该性能监测项目数据报表。

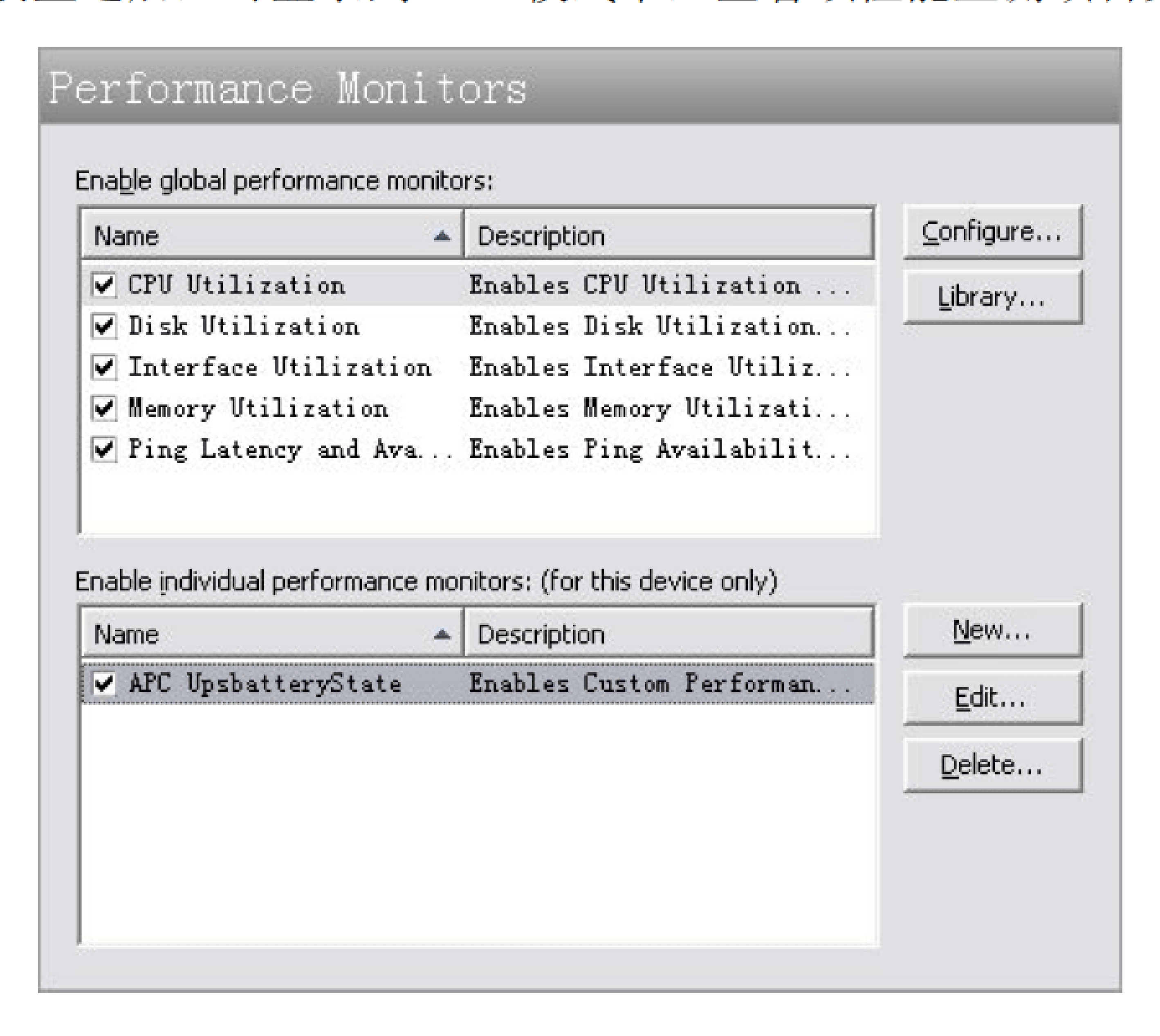


图 7-27　APC UPS 的 MIB 节点实例

7.2.4　WMI 方式监测 SQL Server 服务

有时，存在这样的情况，在监测的其中一个设备中提示进程报警，当试图去解决该故障却发现该设备业务看上去一切运行正常。这种情况有可能是进程导致内存溢出，需要找出报警的原因以及该报警与其他进程之间的关系。那么可以通过对该故障进程建立监测项目，以查找原因解决故障。

本例中，使用 WMI 对服务器中的 SQL Server 服务进程建立监测，并查看该进程使用的内存情况。步骤如下：

（1）选择包含 SQL Server 服务的 Windows 主机设备，并打开其属性 Properties 界面，选择 Credentials 页面，添加访问该主机的凭证。

（2）在 Windows Credentials 列表中，新建或选择能够正确访问该设备的证书，然后单击 OK 按钮，如图 7-28 所示。

（3）为设备添加单独的性能监测对象。在设备属性界面选择 Performance Monitors 页面，并在界面下方的 Enable individual performance monitors 区域，单击 New 按钮。在下拉列表框中，选择通过 WMI 方式 WMI Performance Monitor 监测进程，如图 7-29 所示。然后单击 OK 按钮，进入 WMI 性能监测对象配置。

（4）在 WMI 性能监测配置界面，输入自定义名称和描述信息（如 SqlServer_WMI），如图 7-30 所示。

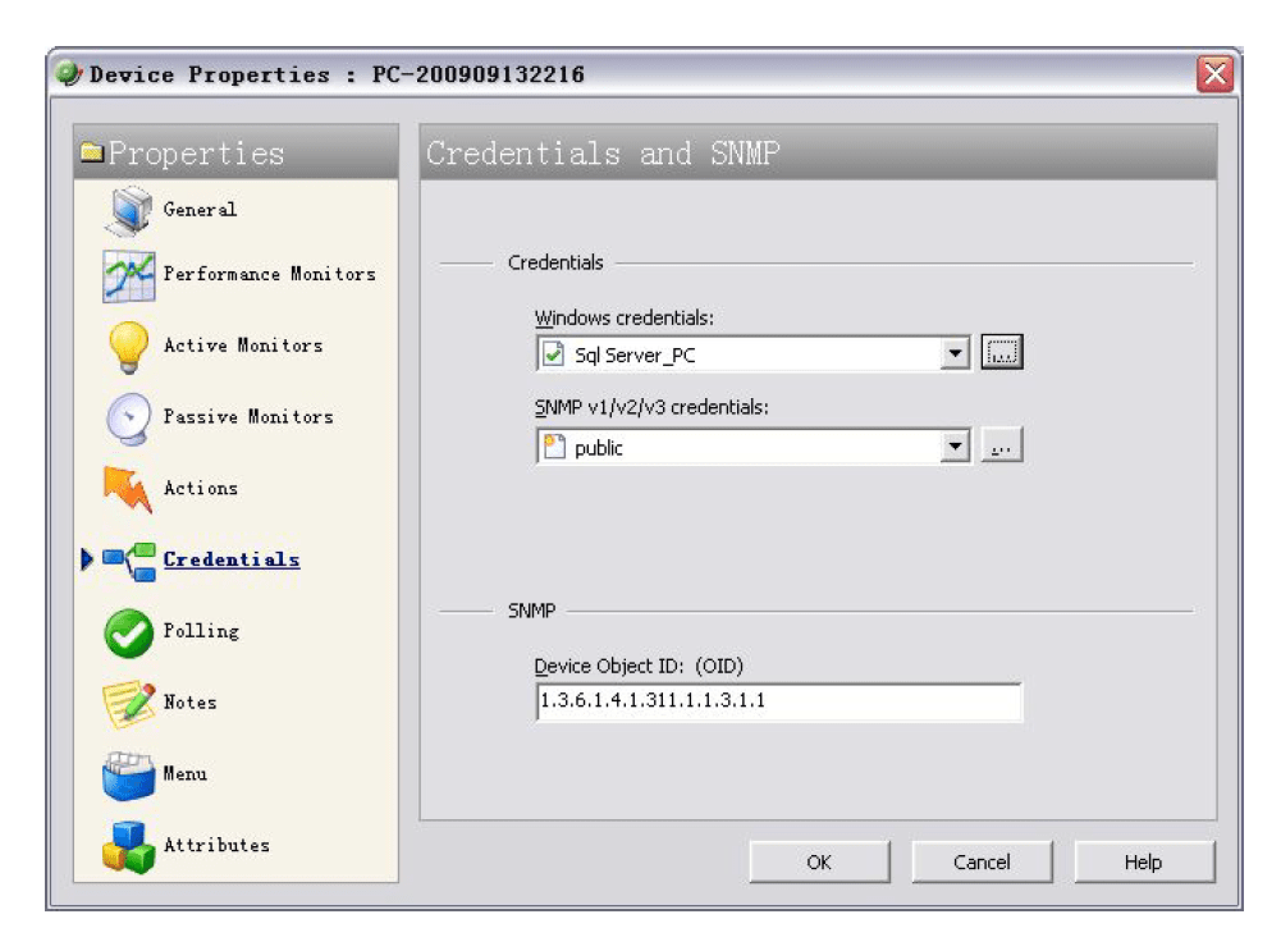


图 7-28 选择 Windows 访问凭证

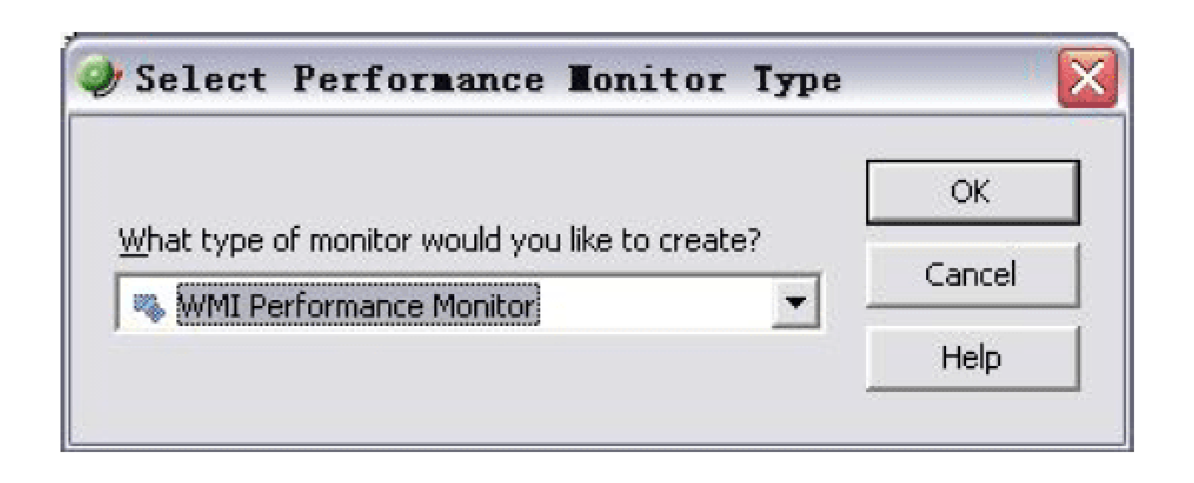


图 7-29 选择新建 WMI 类型监测对象

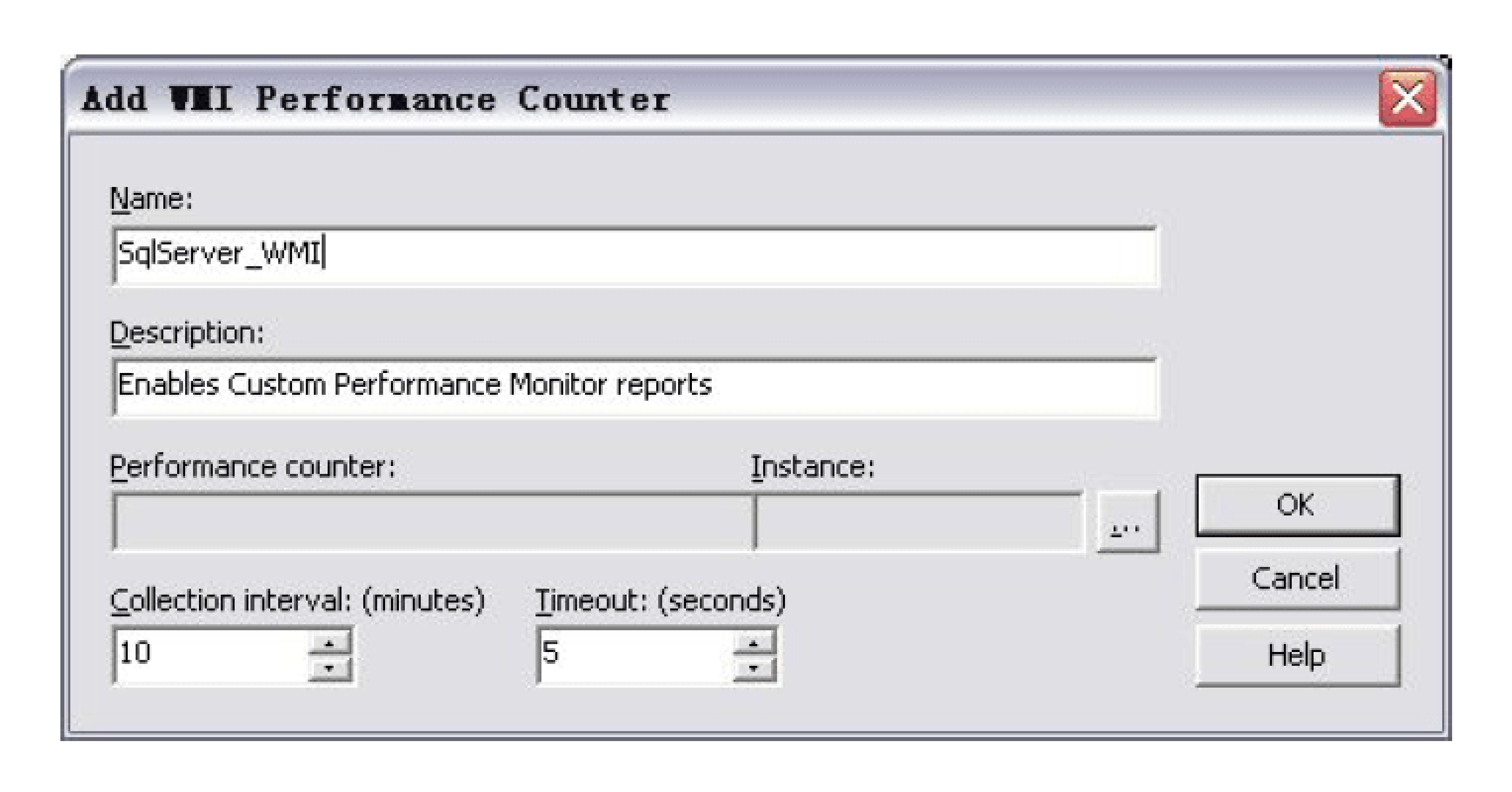


图 7-30 输入 WMI 名称和描述信息

（5）单击 Instance 右边的浏览【...】按钮，打开性能计数器对话框。在左侧的 Performance counter（性能计数器）列表中选择进程项 Process，并在其目录下选择私有字节数 Private Bytes 子选项（私有字节为当前运行在内存中的字节数。在内存中，分配给该进程的字节

数不能被其他进程共享）。此时，对话框右侧区域的 Performance Instances（性能实例）列表中列出了该设备的应用程序。此处选择 sqlserver 选项，如图 7-31 所示。

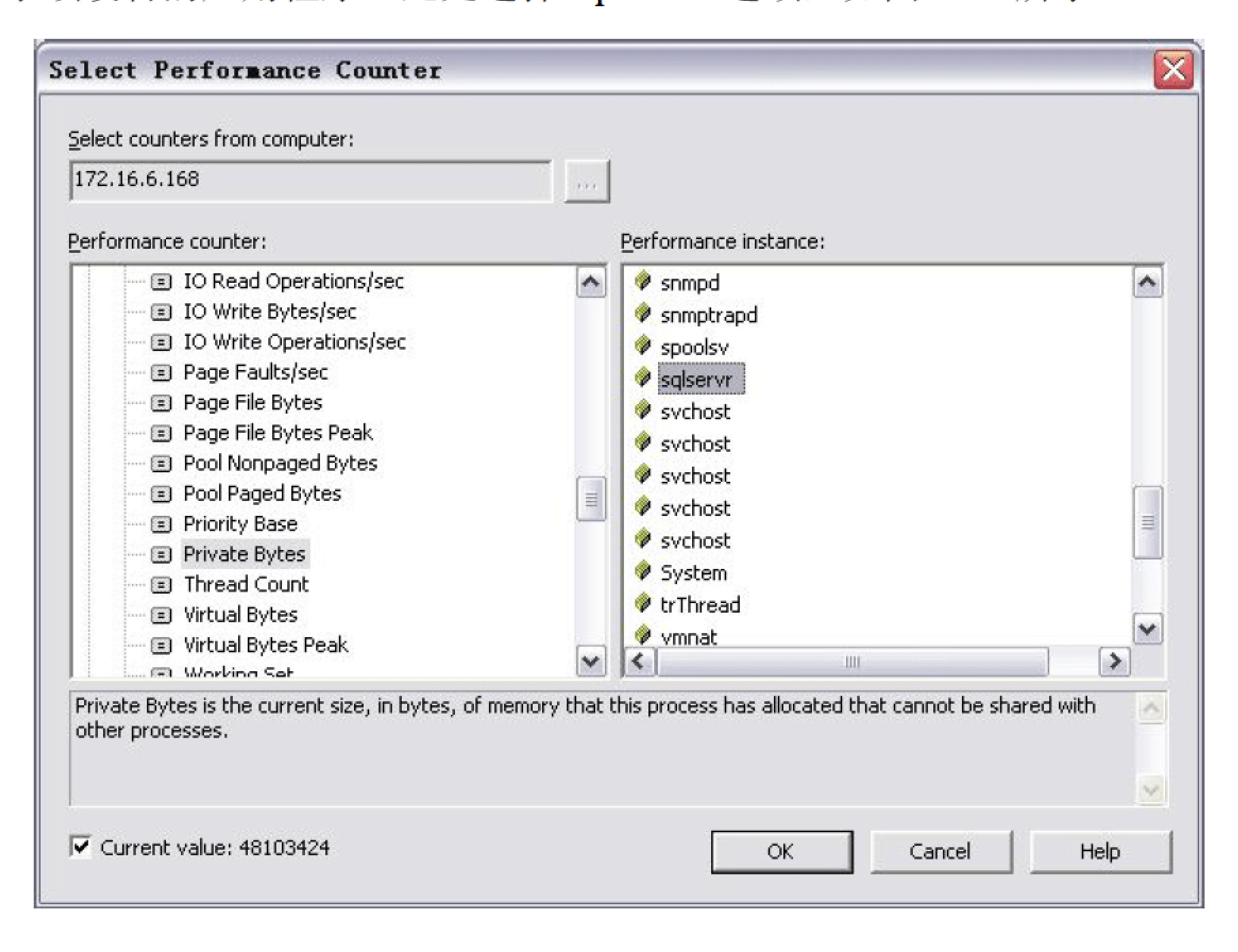


图 7-31 选择 SQL Server 监测对象

（6）选择对象返回后，界面中已经自动添加了性能计数器对象和实例。修改 Collection interval（采集信息的时间间隔）及 timeout（失败时延）后，即添加了计数器和所要监控的程序，如图 7-32 所示。

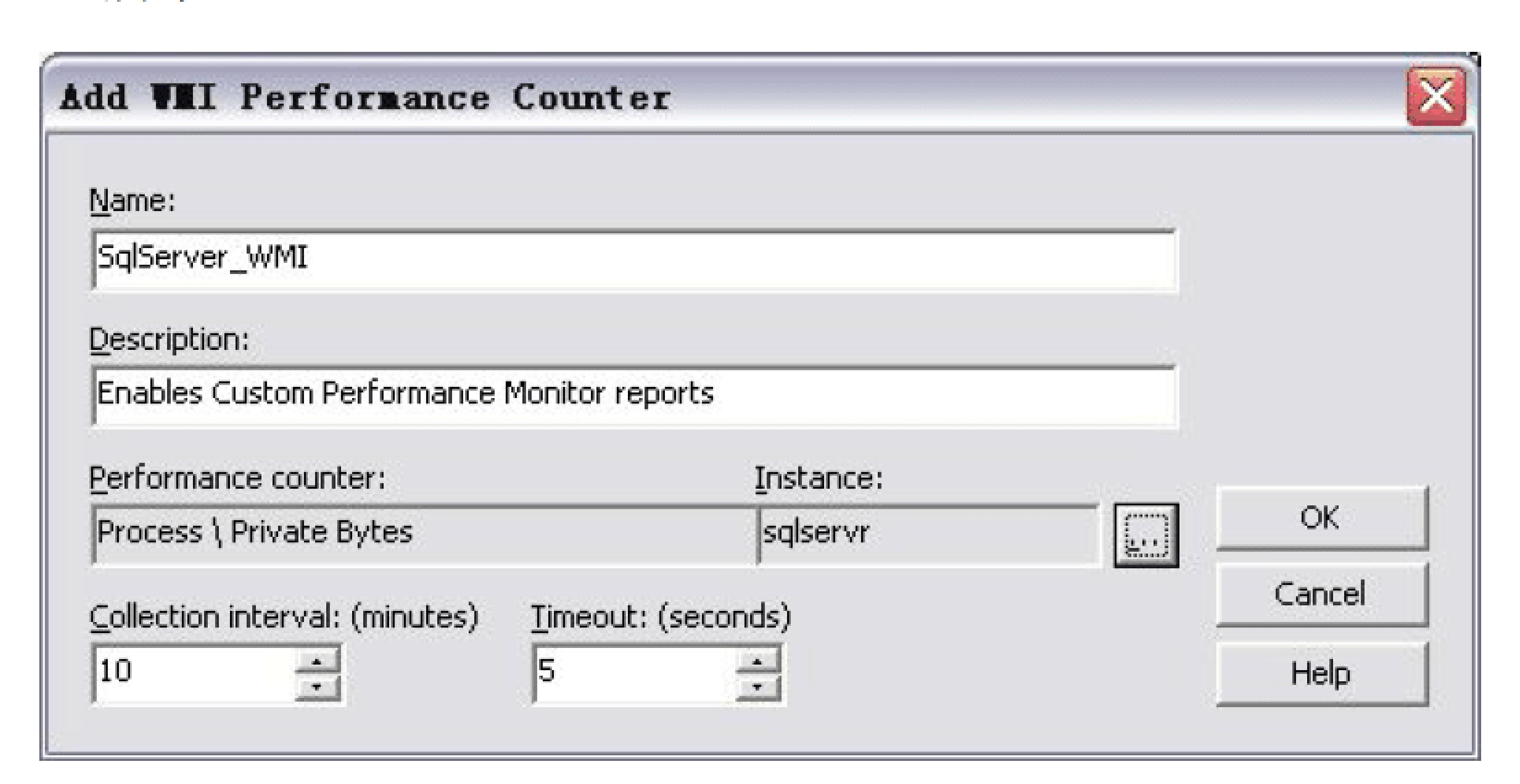


图 7-32 完成 WMI 监测对象配置

注意：此处的时间间隔是针对于该 WMI 监测的轮询时间，对其他监测对象无影响。

（7）在轮询操作采集到足够的数据后，就能够查看性能报表。进入到网页视图中，选择报表 Reports | Device 选项，打开设备的报表清单，然后选择 Custom Performance Monitor

选项，在弹出的报表界面中的左侧 Select Monitor 选择框中，选择刚创建的监测项目，即可看到 SQL Server 程序占用内存情况，如图 7-33 所示。

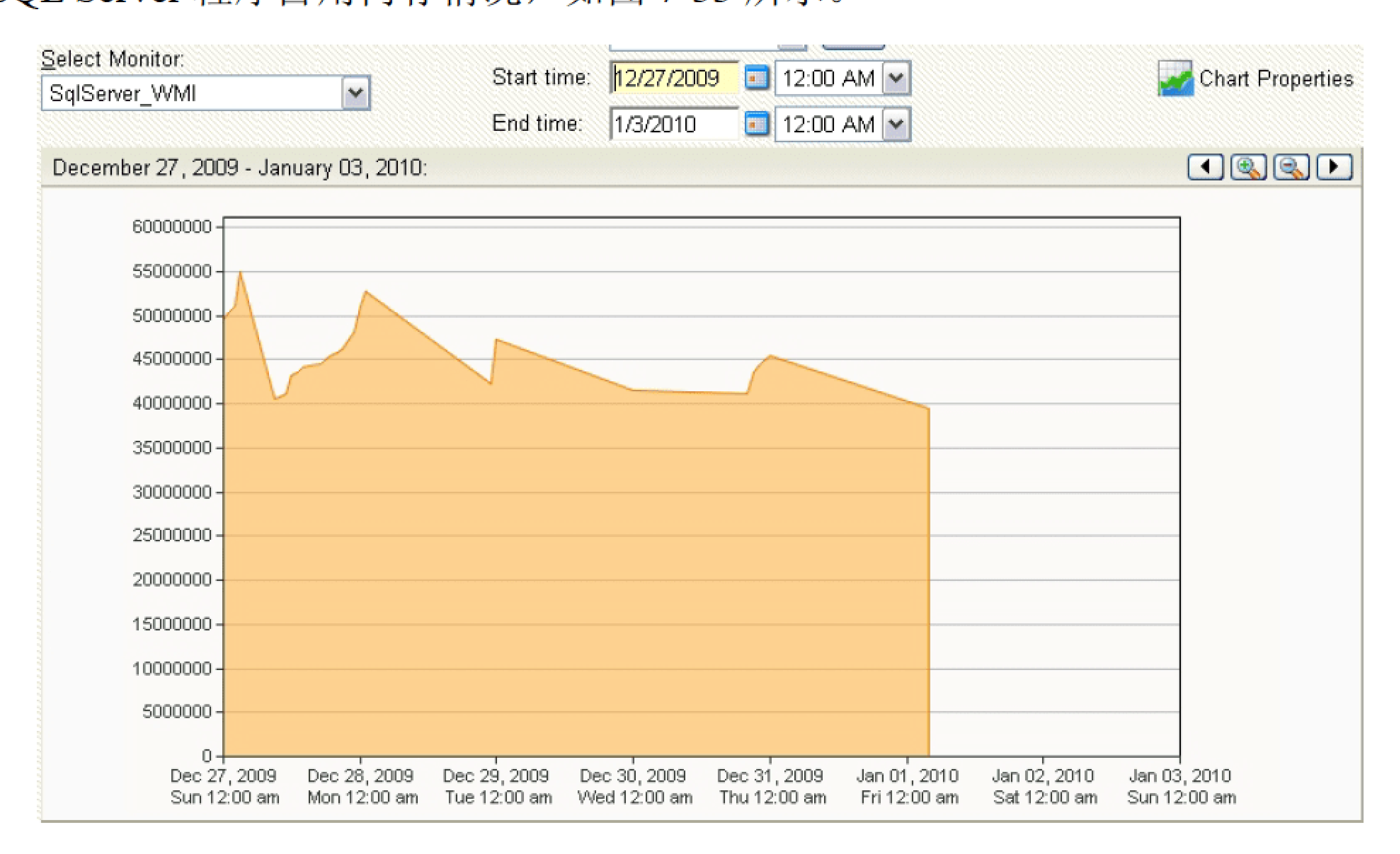


图 7-33　应用程序内存使用情况

通过 SNMP 方式监测机房温度和 UPS 电池运行参数，以及通过 WMI 方式监测 SQL Server 程序占用内存情况的实例讲解，完成了对性能监测方式的介绍。接下来，用实例介绍主动监测方式的应用。

注意：性能监测主要用于设备性能数据的采集，以形成报表或图表，而主动监测主要用于监测异常状态的发生，并触发报警提示动作。

7.3 Active Monitors 主动监测

前面举例讲解了对机房温度建立性能监测项目。监测项目能够按照轮询时间间隔采集温度值并形成报表，在收集了几天性能数据后会发现有偶然的异常温度数值出现。如果想让异常温度出现时发出报警信息，则需要建立一个 Active Monitor，以监测返回的值是否在正常范围内，如果超出设定范围，则触发报警提示。建立步骤如下：

（1）打开 Active Monitor Library（主动监测库）界面，单击 New 按钮，在主动监测类型下拉列表中选择 SNMP Monito 选项，弹出新增 SNMP 监测项目界面，如图 7-34 所示。

（2）选择 Instance 右侧的【…】浏览按钮，在弹出的窗口中输入空调远程接口板的 IP 地址和访问的社区字符串，将连接到接口板，并弹出 SNMP MIB Walker 界面。在 MIB 树中找到上一小节中介绍的空调温度参数，即 Private | emerson 目录下 lgpAcProducts 选项，选择 Object ID 和 Instance 值后返回，参数对象和实例取值如图 7-35 所示。

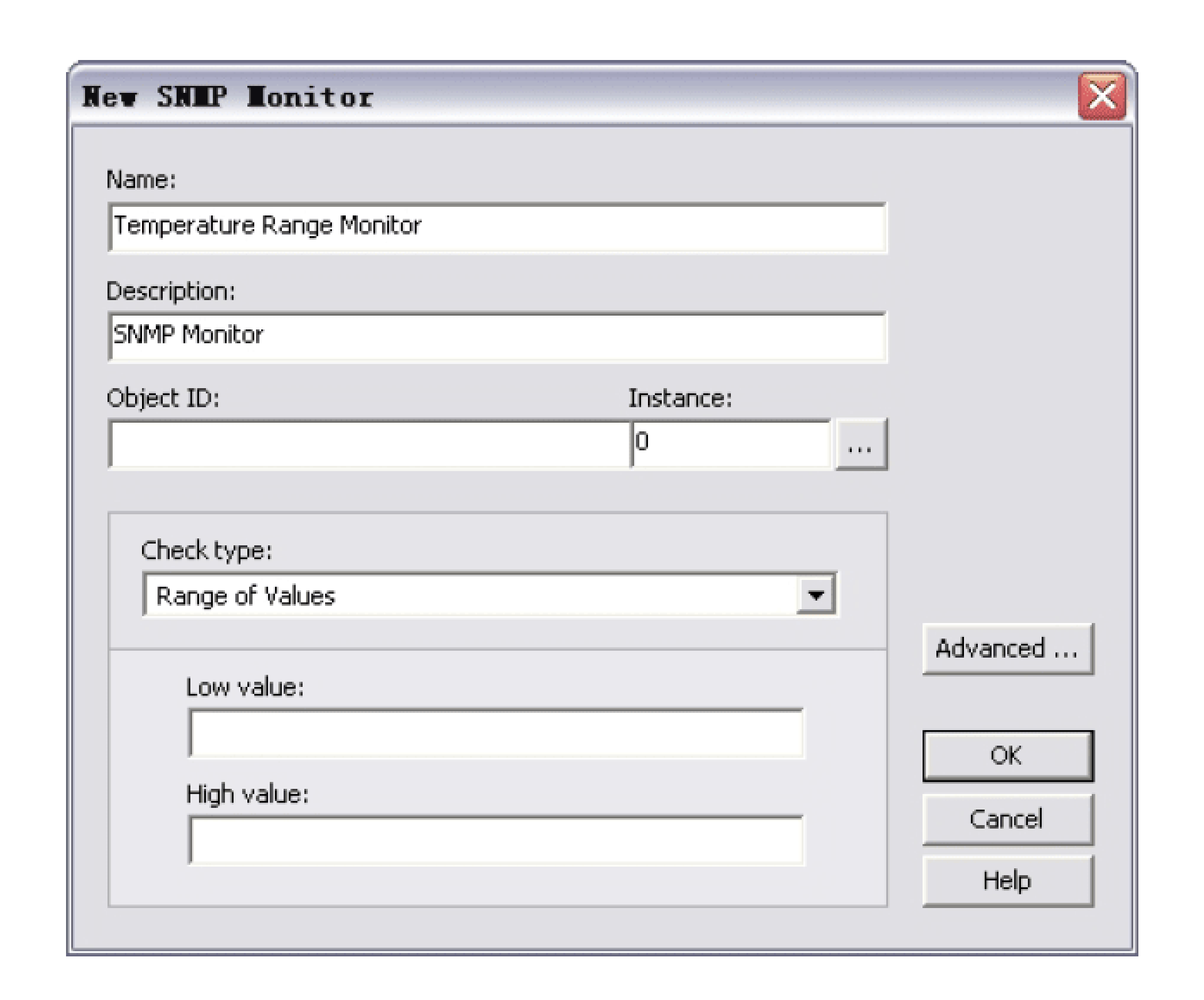


图 7-34　新建 SNMP 监测对象界面



图 7-35　选择监测对象实例

（3）在该界面下方的温度区间阈值框中，是以美国华氏温度 ºF（Fahrenheit temperature scale）为单位，摄氏温度（℃）和华氏温度（F）之间的换算关系为：

ºF=9/5ºC+32 或 ºC=5/9（ºF-32）

如果需要设定报警的区域为小于 16ºF 和大于 25ºC，那么按照公式计算出来的华氏温度值为小于 60.8ºF 和大于 69.5ºC。以 WhatsUp Gold 的规定，还需要在华氏温度基础上再乘以 10 来表示温度区间。那么 Low value 文本框中输入参数 608，在 High value 文本框中输入 695，即完成了温度区间的设置，如图 7-36 所示。

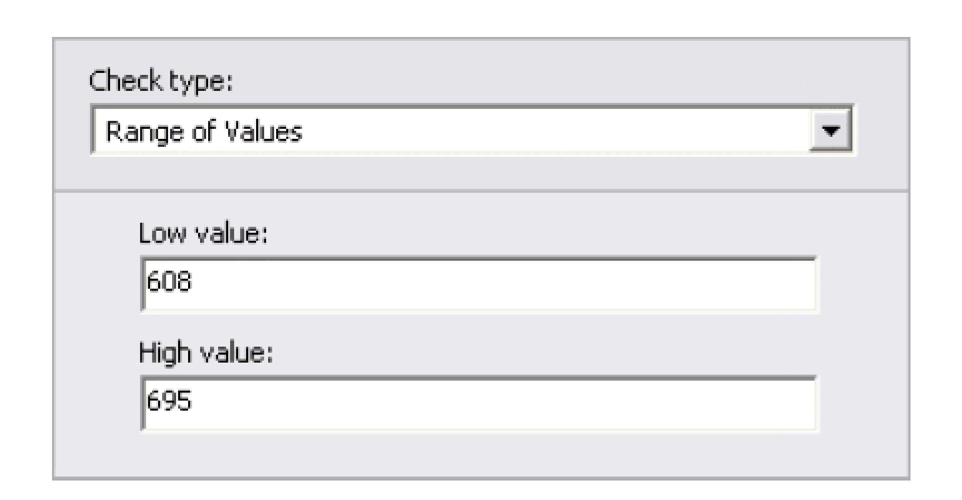


图 7-36　温度区间值

（4）在主动监测库中添加了温度范围监控项目后，即可回到设备列表中选择要监控温度的空调设备对象，并为其添加温度范围的主动监测项目及报警提示动作。一旦监测到的温度超出了规定的温度范围，则 WhatsUp Gold 触发设置的报警提示动作。

7.3.1　WMI 方式主动监测非法入侵

通常，入侵者会通过随机生成的用户名和密码，在网络 IP 地址段范围内使用脚本逐台

暴力破解网络中的计算机，并非法登录到某台计算机中。这种类型的攻击，对于网络中的域用户和存储的重要信息都是极其危险的。所以当此类攻击发生的时候，网络管理员需要立即发现。

通过建立用户自定义的 WMI 主动监测器去监测 Windows 设备的性能计数器，当此类攻击发生，就能够从 WhatsUp Gold 中得到报警信息，以阻止攻击者获取网络中的重要数据。建立 WMI 方式监测非法入侵的步骤如下：

（1）同样，在为设备建立 WMI 方式的主动监测项目之前，先为设备选择 Windows 登录访问凭证。

（2）打开域服务器属性界面，选择 Active Monitors 页面，并单击 Add 按钮添加监测对象。在默认的下拉列表中，并没有包含 WMI 监测项目，可通过单击下拉列表右边的浏览【...】按钮打开主动监测库进行 WMI 监测的添加。在主动监测库中，单击 New 按钮，将弹出类型选择提示框，如图 7-37 所示。

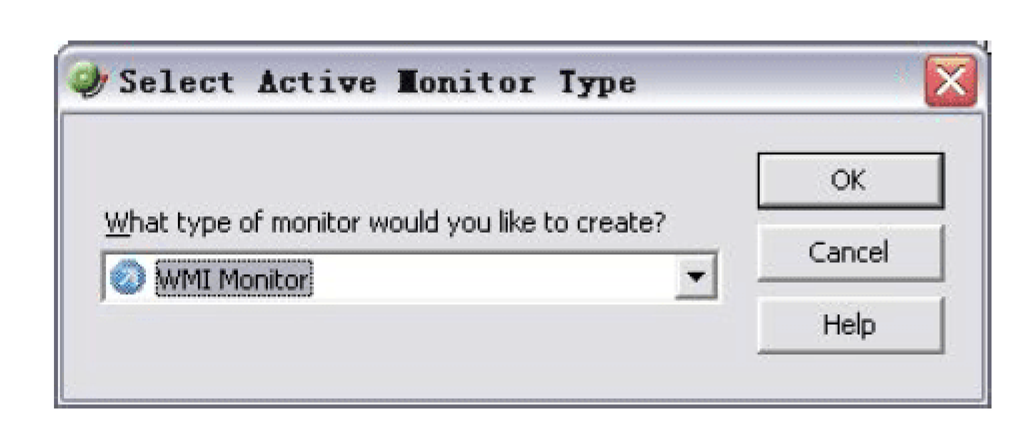


图 7-37　选择新建主动监测类型

（3）在此，选择 WMI Monitor 选项以监测暴力破解方式的非法登录。将该监测项目命名为 ErrorsLogon，然后单击 Instance 右边的【...】浏览按钮，打开性能计数器对话框。在对话框的 Performance counter 列表中选择 Server | Errors Longon 选项，作为非法登录监测对象，如图 7-38 所示。

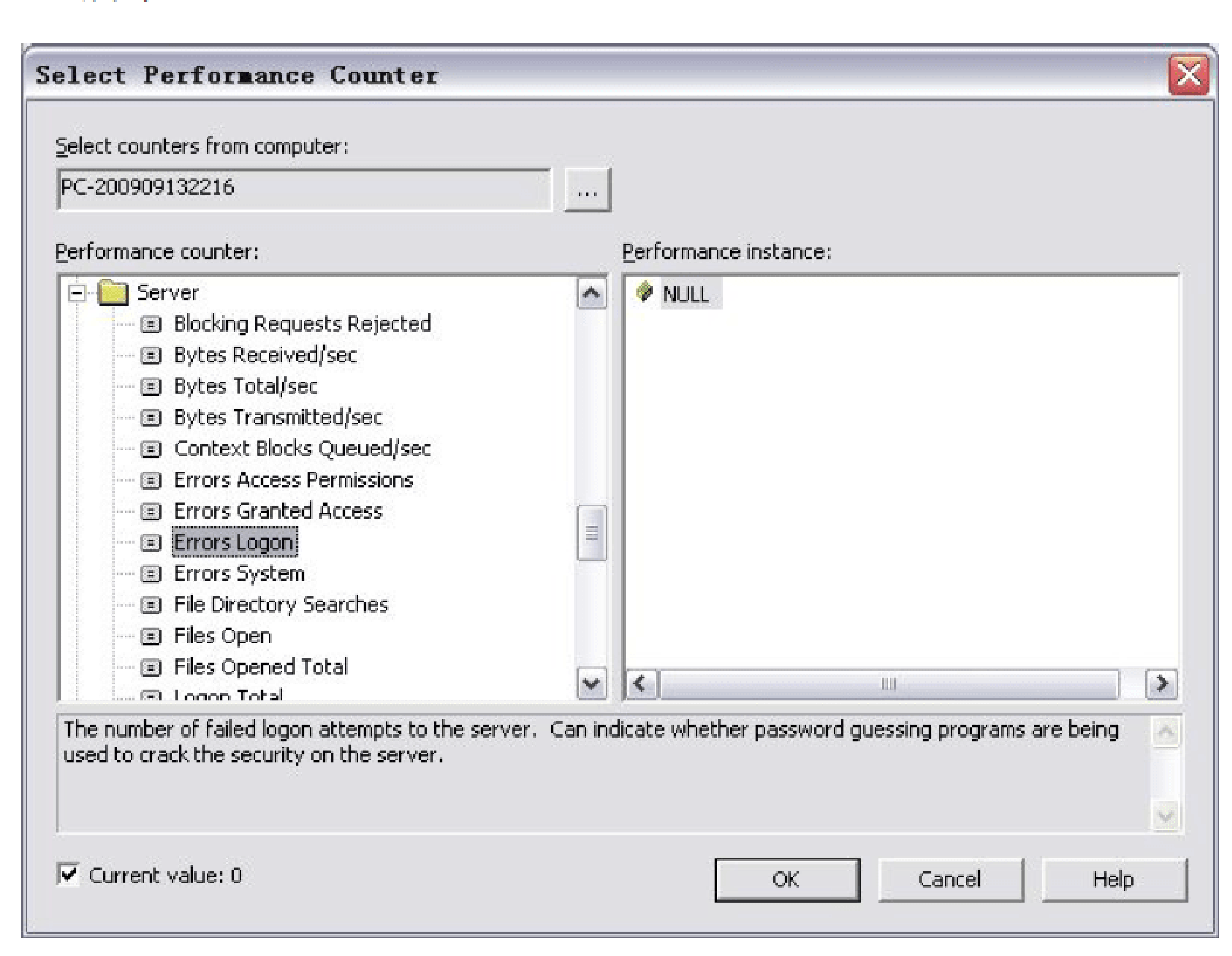


图 7-38　选择登录的实例对象

（4）选择 WMI 计数器对象后，返回 WMI Monitor 设置界面，选择 Check Type 选项，其中有如下 3 种检查类型。

- ❑ Constant Value：常量值，即输入认为可以登录失败的次数，输入 4，那么连续 4 次登录错误，则认为是非法入侵。
- ❑ Range Of Value：区间值，即在一个变化区间内，如果错误登录的次数在该区间内，认为是入侵并触发报警。
- ❑ Rate Of Change：变动率，是描述错误登录尝试的变动情况。

此处选择常量值 Constant Value 选项，数值为 5，然后将 If the value matches，then the monitor is 选项状态选择为 Down，即当错误登录次数达 5 次时，该监测项目状态变为 Down，触发告警信息，如图 7-39 所示。

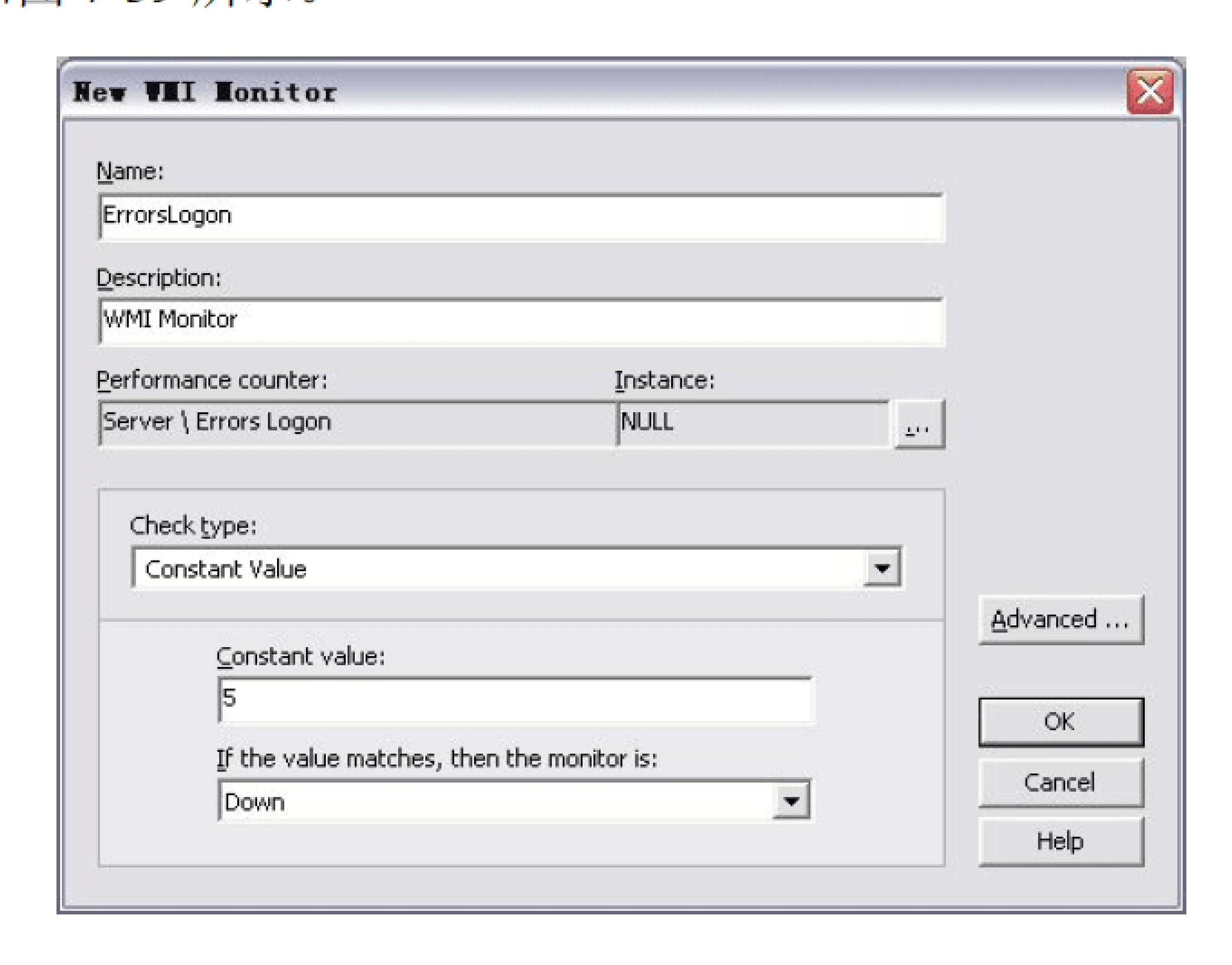


图 7-39　设置非法登录监测完毕

（5）保存该 WMI 监测项目后，返回到选择监测类型界面，在类型下拉列表中可以看到已经包含了之前新建的 WMI 监测项目，如图 7-40 所示。

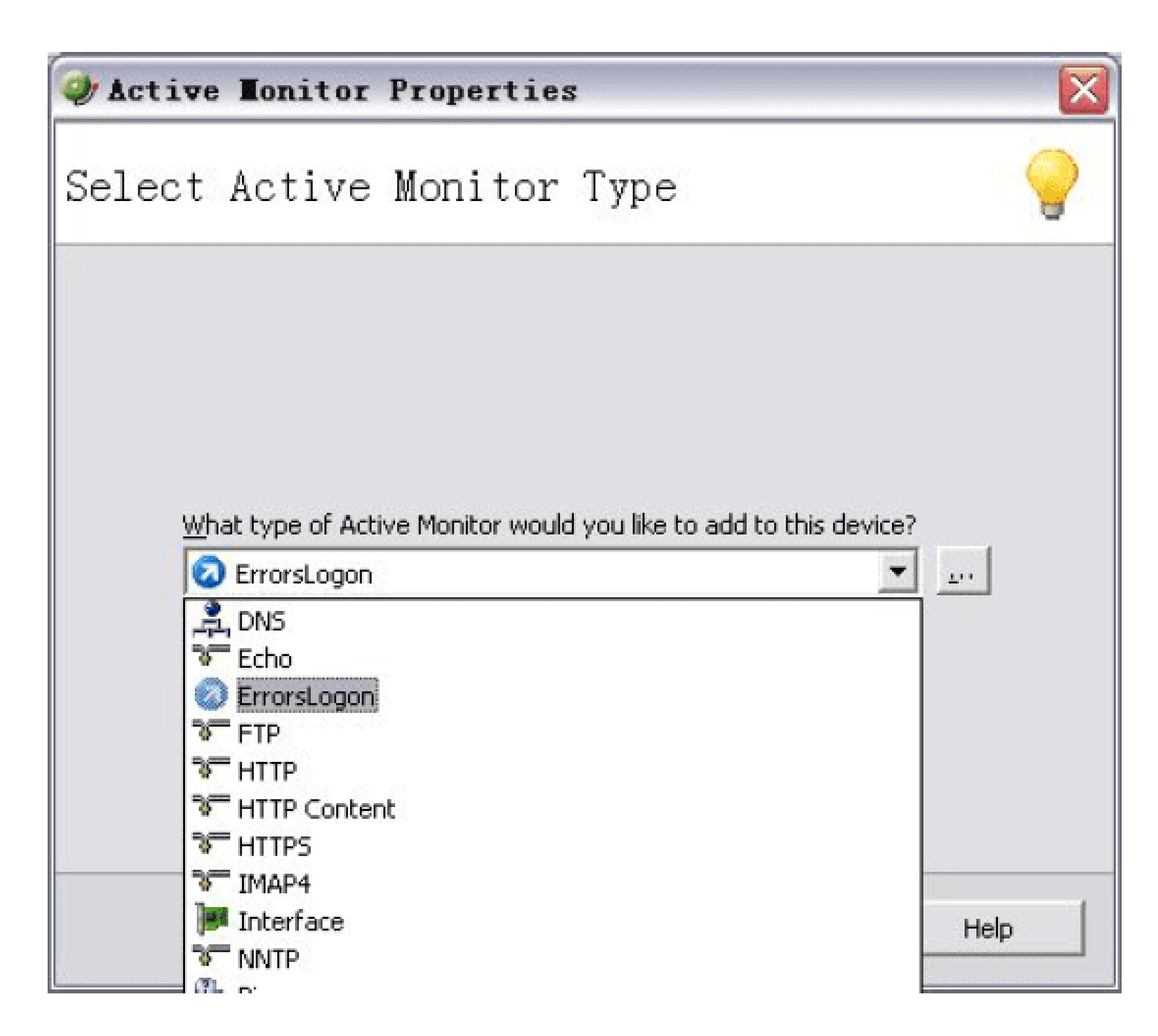


图 7-40　新建非法登录的主动监测对象

（6）选择该监测项目，然后为该监测选择报警提示动作。设置完成后，在 Active Monitors 页面能够看到刚才建立的 ErrorLogon 监测项目，如图 7-41 所示。

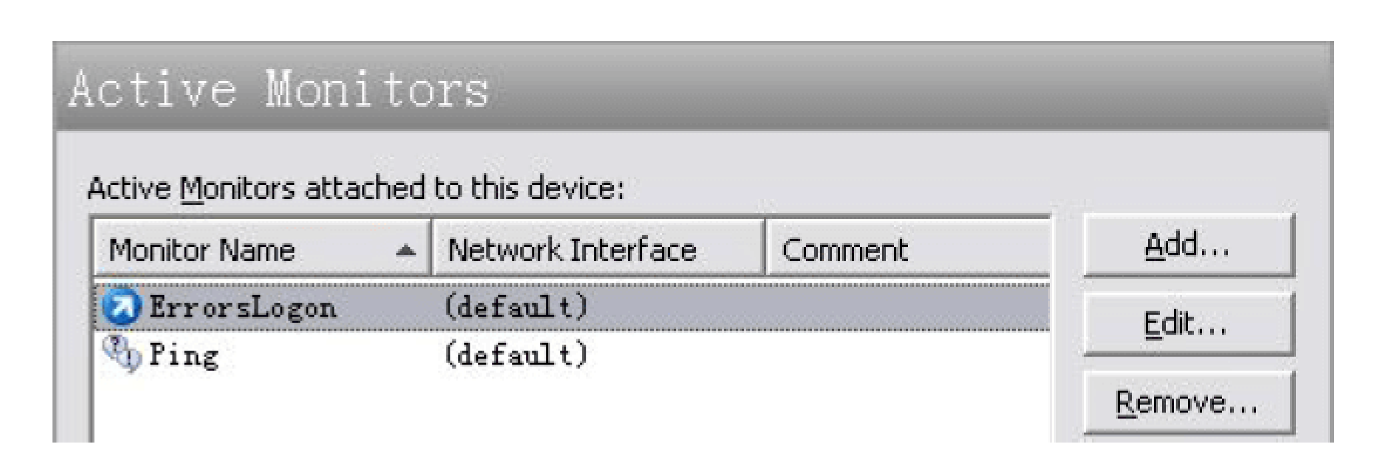


图 7-41　新建非法登录主动监测完毕

此时，如果对该 Windows 主机非法登录尝试超过 5 次时，WhatsUp Gold 将根据设置的提示动作进行报警提示。

7.3.2　SNMP 方式主动监测邮件服务

1．Exchange Server 介绍

Microsoft Exchange Server 即微软消息通信与协作服务器，它实现与客户端应用程序协同管理网络邮件、日程表和即时通信服务。

Exchange Server 是网络中提供发送和接收电子邮件服务的系统。它除了提供全部邮件服务功能外，还提供共享的日程管理、任务管理，支持基于移动电话和网页等方式获取邮件信息，以及支持大容量的数据存储。同时，提供了客户端应用程序（例如 Microsoft Outlook）作为连接邮件服务器的客户端收发程序。客户端程序通过个人电脑或移动电话，连接存储电子邮箱的服务器接收电子邮件，并通过邮箱服务器连接至 Internet 将邮件转发到其他用户邮箱。

2．Exchange Server 版本

Exchange Server 服务器有两种版本，标准版和企业版。标准版包括 Active Server、网络新闻服务和一系列与其他邮件系统的接口；企业版除了包括标准版的功能外，还包括与 IBM OfficeVision、X.400 等协议通信的网关接口。

应用程序版本中，Microsoft Exchange 2000 为较老版本，用户量已经较少。目前较为主流的 Microsoft Exchange Server 应用程序版本包括如下 3 个，特点分别介绍如下。

- Microsoft Exchange 2003：具有高度生产力和面向移动访问的理想消息和协作服务器平台。提供了丰富的客户端功能协同工作。可提供具有安全性和隐私性的移动、远程和桌面电子邮件访问。提供基于电子邮件的协作以及轻松地升级、部署和管理。
- Microsoft Exchange Server 2007：Exchange Server 2003 的下一个版本，增加了许多新的特性和功能以满足多数组织、企业的不同需求，为计算机网络中的 E-mail 和其他形式的交互通信内容的收发工作提供平台支持，该平台被设计成可以和多种客户端软件进行交互，为最终用户提供更多访问方式连接到邮箱。

- Microsoft Exchange 2010：相对之前版本主要改进了 3 个方面，灵活可靠性、随时随地获取、保护和遵从，增加类似于 Gmail 里的会话模式（'conversation view'）的支持，同时还完整支持各种网页浏览器，整合 IM 和 OCS 通信。提供了简化通过提高业务的移动性，增强了可靠性和性能。

7.3.3 详解 Exchange 服务

Exchange 服务器包含多项重要的服务，服务器上必须执行这些重要的服务，才能保证邮件系统的正常运行。在网管程序中，可针对这些服务进行监测，以了解邮件服务的正常运行。

1. Info Store 信息存储服务

Exchange Information Store 服务是 Exchange 系统中一个非常重要的组件。该服务实现了 Exchange 存储，它管理 Exchange 的存储区域，维护用户邮件资料库，控制了对邮箱和公共文件夹数据库的操作请求。该服务执行文件为 Store.exe，执行程序位于\Program Files\Exchsrvr\Bin 目录中。

2. Site Replication（Exchange SRS）站点复制服务

安装 Exchange Server 时，可以采用原始模式和混合模式。原始模式就是在网络中仅使用一个版本的一台 Exchange Server 服务器。而混合模式允许在网络中存在多个不同版本的 Exchange Server。在混合模式下，SRS 就提供了 Exchange 5.5 和 Exchange 2000 或 Exchange 2003 之间的目录同步和邮件复写。

SRS 充当了 Exchange 多个站点之间的目录复制服务器。在运行 SRS 的 Exchange 混合模式网络中，通过 Exchange 系统管理员可以查看并判定邮件服务器中哪个 Exchange Server 正在执行 MSExchangeSRS 服务。在原始模式下，并不需要安装此服务。

3. Management 系统管理服务

Management 服务时在 Exchange 2000 Server（SP2）及以上版本中出现的新 Exchange 管理服务，该服务为必须启动项。Management 使用 WMI 来实现 Exchange 的信息管理。它同时也是一个 WMI 管理应用程序，可通过命令方式获取 Exchange 对象信息或控制修改信息。如果停止此服务，则通过该服务实现的 WMI 提供程序（如邮件跟踪和目录访问）将无法正常工作。

4. Exchange MTA 传输代理服务

Exchange 邮件传输代理（MTA）是 Exchange Server 2003 的核心组件，它负责所有非 SMTP 的邮件传输。如果网络中使用 RPC（远程过程调用）连接器或 X.400 连接器连接了外部 X.400 邮件系统，同时连接了 Exchange 邮件系统，则有可能使用 MAT 作为 X.400 邮件系统和 Exchange 服务器之间的邮件传输模式。MTA 还可以处理来自其他邮件系统邮件

或发送到其他邮件系统（例如 Lotus cc：Mail、Lotus Notes、Domino 、Novell GroupWise 和 Microsoft Mail）邮件。

MAT 服务在混合模式环境（即邮件在 Exchange Server 5.5 与 Exchange Server 2003 或 Exchange 2000 Server 不同站点之间传递）中的作用尤为重要，MAT 提供不同站点之间的连接和互访。此外，连接 x.400 和其他邮件系统都需要 MTA，如图 7-42 所示。

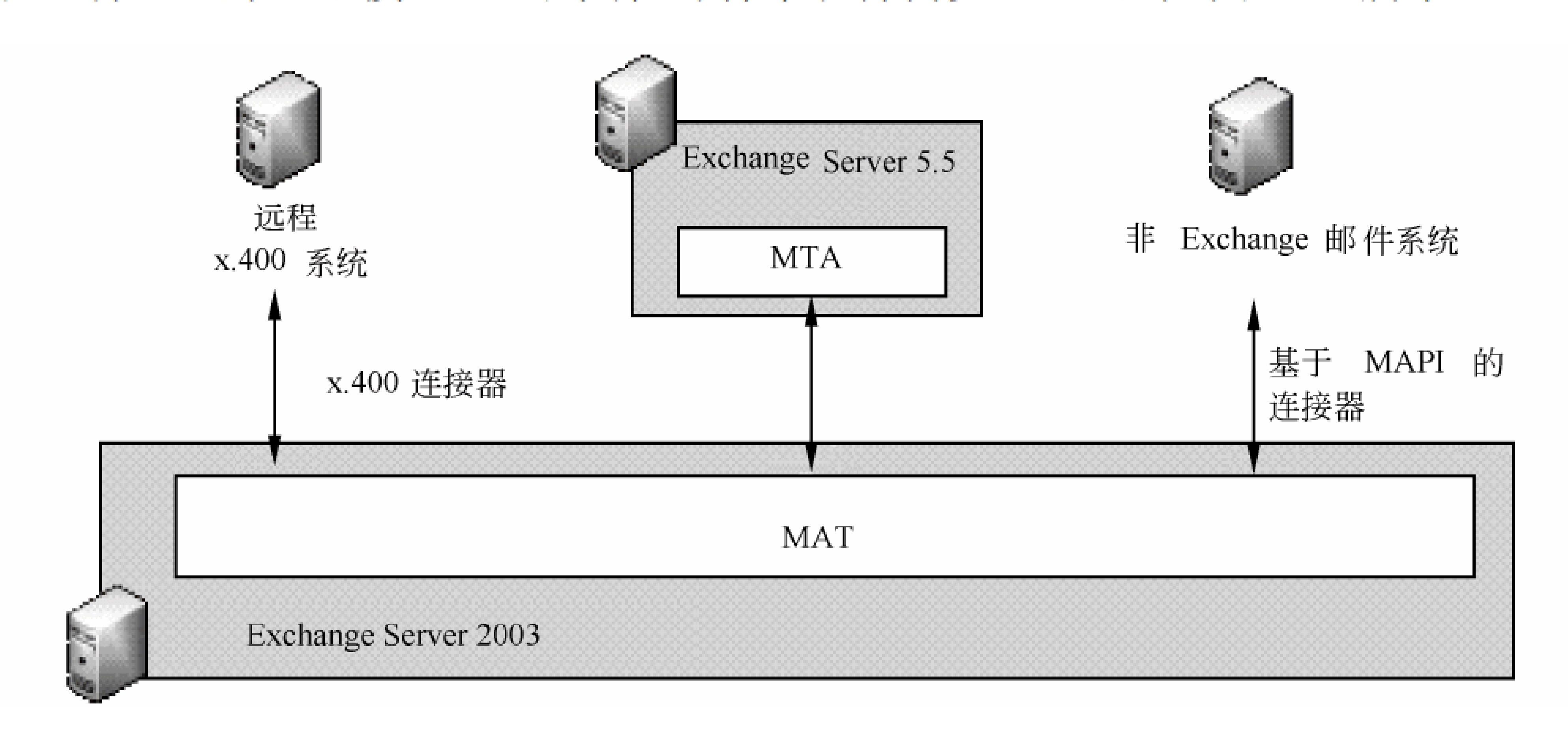


图 7-42 MTA 体系机构

5. System Attendant 系统维护服务

所有的 Exchange 核心服务都需要 System Attendant 服务。该服务提供监视、维护和 Active Directory（活动目录）查找等维护。例如，监视服务和连接器、监视端口通信、生成代理、从 Active Directory 复制到数据库、发布忙/闲信息、维护邮箱等。如果停止此服务，则监视、维护和查找服务都不可用，为邮件服务器的必要服务项。

6. Routing Engine 路由引擎

Routing Engine 路由引擎为运行 Exchange 2003 的服务器提供拓扑结构和路由信息，同时避免邮件在不同服务器之间反复传送的回环问题。如果停止此服务，则邮件服务器在传输邮件时无法选择最佳路由。

7. POP3 邮件接收服务

POP（Post Office Protocol，邮局通信协议），互联网上的一种通信协议，是 TCP/IP 协议族中的一员，主要功能是用于接收电子邮件。POP3 是邮局协议的第 3 个版本，使用 TCP 的 110 端口，主要规定了用户可远程管理和接收服务器上的电子邮件，允许用户从服务器上收取邮件存储到本机，同时删除远程邮件服务器上的邮件。

当发送一份 E-mail 到指定邮箱时，邮件服务器必三接收并保存这封邮件。当邮件接收者需要收取邮件的时候，就必须通过 POP3 通信协议，才能取得邮件，如图 7-43 所示。

8. IMAP4 邮件接收服务

IMAP（Interactive Mail Access Protocol，交互式邮件存取协议）同样是一种基于 TCP/IP

协议之上的邮件获取协议，常用的版本是 IMAP4，使用的端口是 143。邮件客户端（例如 MS Outlook Express）可通过这种协议从邮件服务器上获取邮件的信息和内容。

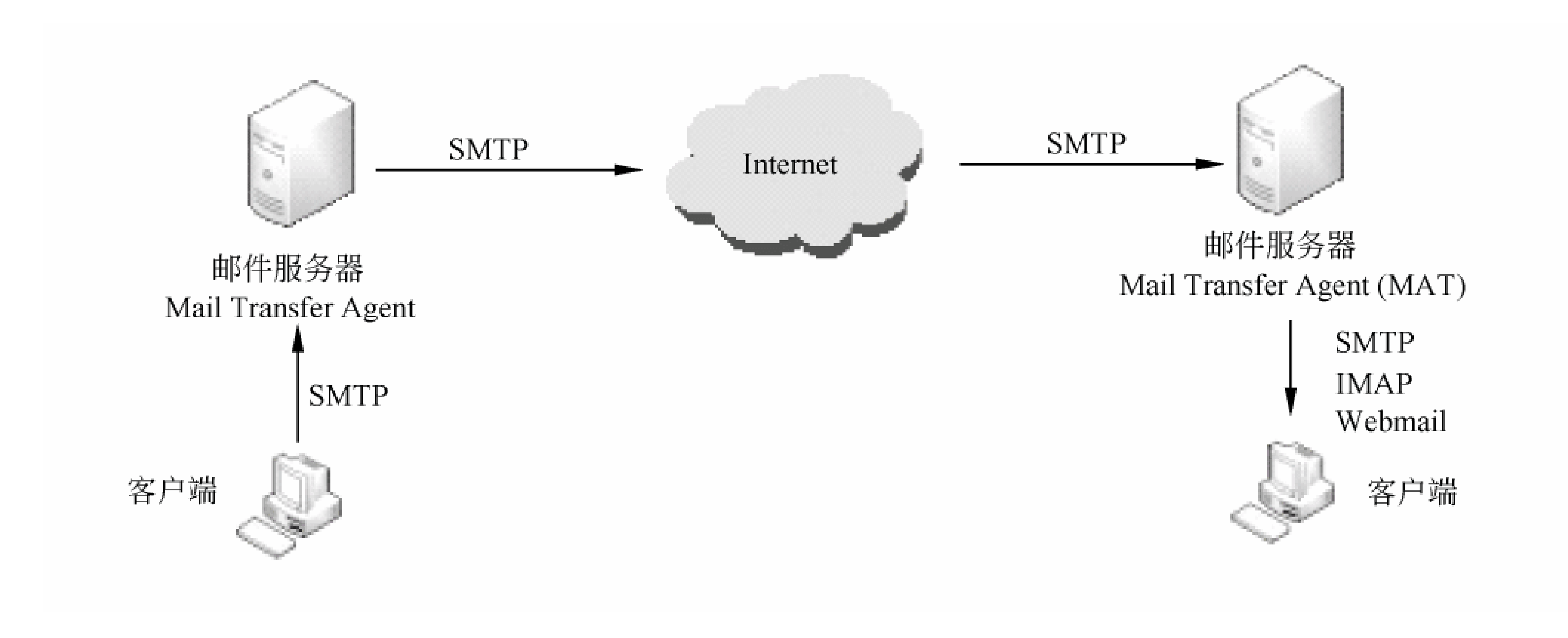


图 7-43　邮件发送和接收流程

与 POP3 协议类似，IMAP 也是提供面向用户的邮件收取服务。但 IMAP4 除了提供 POP3 功能之外，还提供了更多的操作，例如通过信件头来决定是否收取、删除邮件，支持邮件内容检索、创建或更改文件夹及邮箱，支持脱机操作和联机操作模式等。它为用户提供了邮件接收的可选择性、远程信息处理和信箱共享功能。

它与 POP3 协议的主要区别是用户可以通过客户端直接对服务器上的邮件进行操作，而不用把所有的邮件全部下载。而 POP3 支持用户从服务器上接收邮件到本机，同时删除远程服务器上的邮件。

9．SMTP 邮件传送服务

SMTP（Simple Mail Transfer Protocol，简单邮件传输协议），用于可靠高效地传送邮件。它定义了将邮件从源地址发送到指定目的地址，控制邮件的中转和传送方式。SMTP 协议属于 TCP/IP 协议族，在邮件发送过程中，SMTP 为邮件发送或中转查找到下一个目的地，并不断传送到最终的 Email 接收地址。

SMTP 重要特性之一是其能跨越异构网络传输邮件，也就是传输“中继”或“网关”的功能，其传输邮件过程中使用 TCP 协议 25 端口，用于监听发送请求和监听请求。

SMTP 是工作在两种情况下：一是将电子邮件从客户端传输到服务器；二是从某一个邮件服务器传输到下一个邮件服务器。同时，又可将 SMTP 协议分为接收和发送两项主要功能，其发送和接收邮件会话是靠发送请求命令和接收响应来完成的。在通信链路建立后，发送 SMTP 发送请求指令至接收 SMTP，若接收 SMTP 能够接收邮件则作出肯定的应答，然后发送 SMTP 继续发出 RCPT 命令以确认邮件是否收到，如果接收到就作出 OK 的应答，否则就发出拒绝接收应答，如图 7-44 所示。

10．X.400 传输协议

Exchange Server 2003 使用 SMTP 协议和 MTA（邮件传输代理）来传输电子邮件，同时支持 X.400 邮件传输标准协议。X.400 最初是在 20 世纪 80 年代由电信公司开发的，并得到国际电话和电报咨询委员会的认可。X.400 协议较为复杂，与 SMTP 协议相比，SMTP

具备更多的功能，例如地址校验、有效性检验、信息头数据插入等，都比 X.400 更具备广泛的应用。

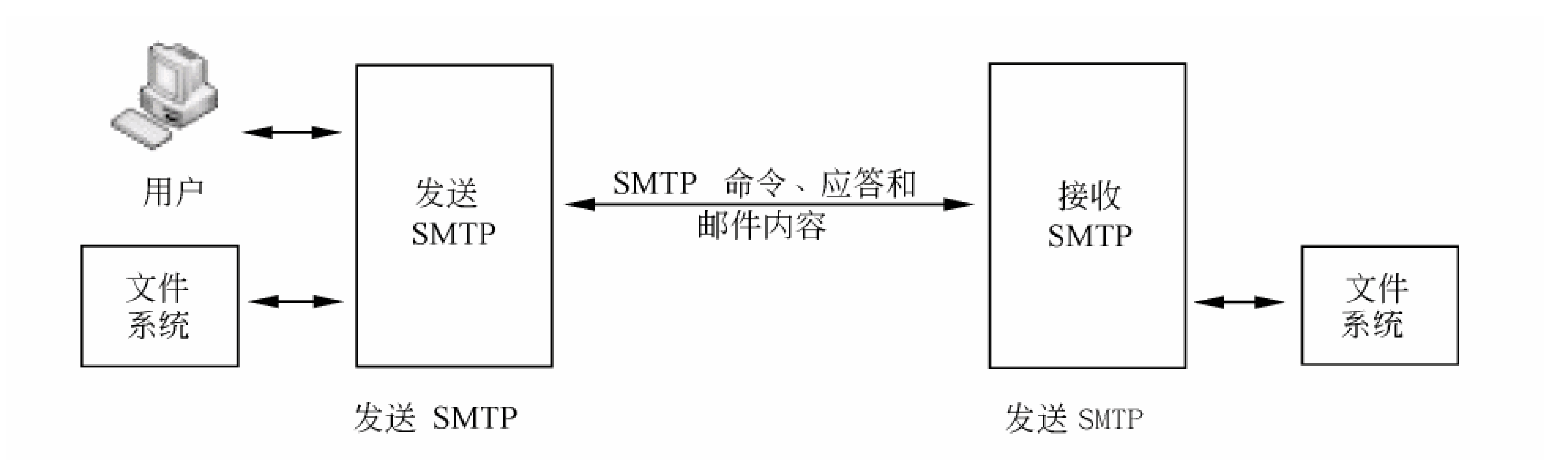


图 7-44　SMTP 使用模型

Exchange 服务器可以使用 X.400 连接器建立 Exchange 结构的邮件传输规则，或用于连接到外部的 X.400 邮件服务系统。所以，在 Exchange Server 2003 企业版中可以创建两种类型的连接器：TCP X.400 连接器和 X.25 X.400 连接器。

11．Exchange 邮件服务器常用端口列表（表 7.1）。

表 7.1　Exchange 邮件服务常用端口列表

协　议	端　口	描　述
SMTP	TCP：25	SMTP 服务使用 TCP 端口 25
DNS	TCP/UDP：53	DNS 监听端口 53
LSA	TCP：691	Exchange Routing Engine 服务通过此端口监听路由链接状态等信息
LDAP	TCP/UPD：389	用于 Active Directory（活动目录）服务所使用的 LDAP（轻型目录访问协议）及 Active Directory 连接器
LDAP/SSL	TCP/UDP：636	SSL（安全套接字层）上的 LDAP 服务端口
LDAP	TCP/UDP：379	用于 SRS（站点复制服务）
IMAP4	TCP：143	用于 Internet 邮件访问协议（IMAP）
IMAP4/SSL	TCP：993	用于 SSL 上的 IMAP4 协议
POP3	TCP：110	用于邮局协议版本 3（POP3）
POP3/SSL	TCP：995	用于 SSL 上的 POP3 协议
NNTP	TCP：119	用于 NNTP（网络新闻传输协议）
NNTP/SSL	TCP：563	用于 SSL 上的 NNTP 协议
HTTP	TCP：80	用于 HTTP 服务
HTTP/SSL	TCP：443	用于 SSL 上的 HTTP 服务

7.3.4　监测 Exchange Server 服务

网络管理员要监测 Exchange 服务器运行状态，可以通过监测 Exchange 中使用的协议和提供的重要服务，或者监测服务器性能的使用情况，以了解 Exchange 业务层面和主机性能的状态。通过监测邮件提供的各项服务，能快速定位故障原因和排除故障。例如，可监

测 SMTP 邮件发送队列的性能是否在预期合理的区间，如果不是，可以及时做出调整防止 SMTP 服务的停止。还可监测服务协议，如 SMTP、POP3 等。

以下通过实例介绍使用 WhatsUp Gold 添加 Exchange 的服务监测。针对邮件服务器，WhatsUp Gold 的主动监测库已经包括了对 SMTP、POP3、IMAP4 和 DNS 服务的监测项目，只需要直接添加即可。步骤如下：

（1）在设备列表中选择 Exchange 服务器，打开其属性界面，并选择 Active Monitors 页面。如果最初使用 SNMP 智能扫描添加设备时，邮件服务器中 POP3、SMTP 等服务运行正常并响应了扫描请求，那么 WhatsUp Gold 能够自动添加对这些服务的主动监测，如图 7-45 所示。

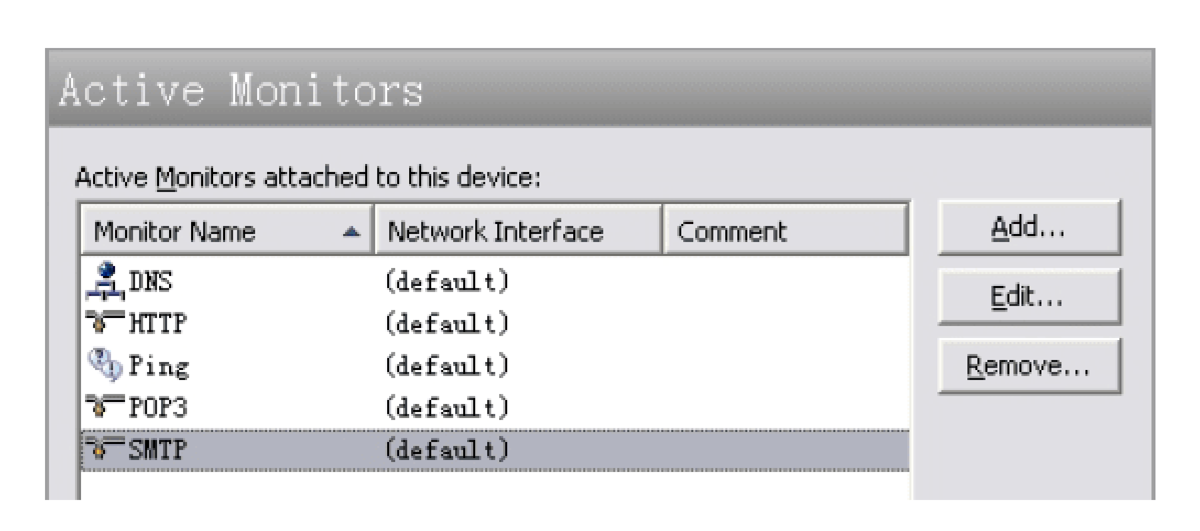


图 7-45　邮件服务器所提供的服务

注意：如果在最初查找设备时未发现以上服务，那么此处可单击 Discover 按钮，程序将重新自动扫描该设备提供的服务，并添加主动监测项目。

（2）如果 WhatsUp Gold 未发现这些服务，需手动进行添加，此处选择添加 SMTP 监测。单击 Add 按钮，打开新增对话框，然后在类型下拉列表中选择 SMTP，如图 7-46 所示。

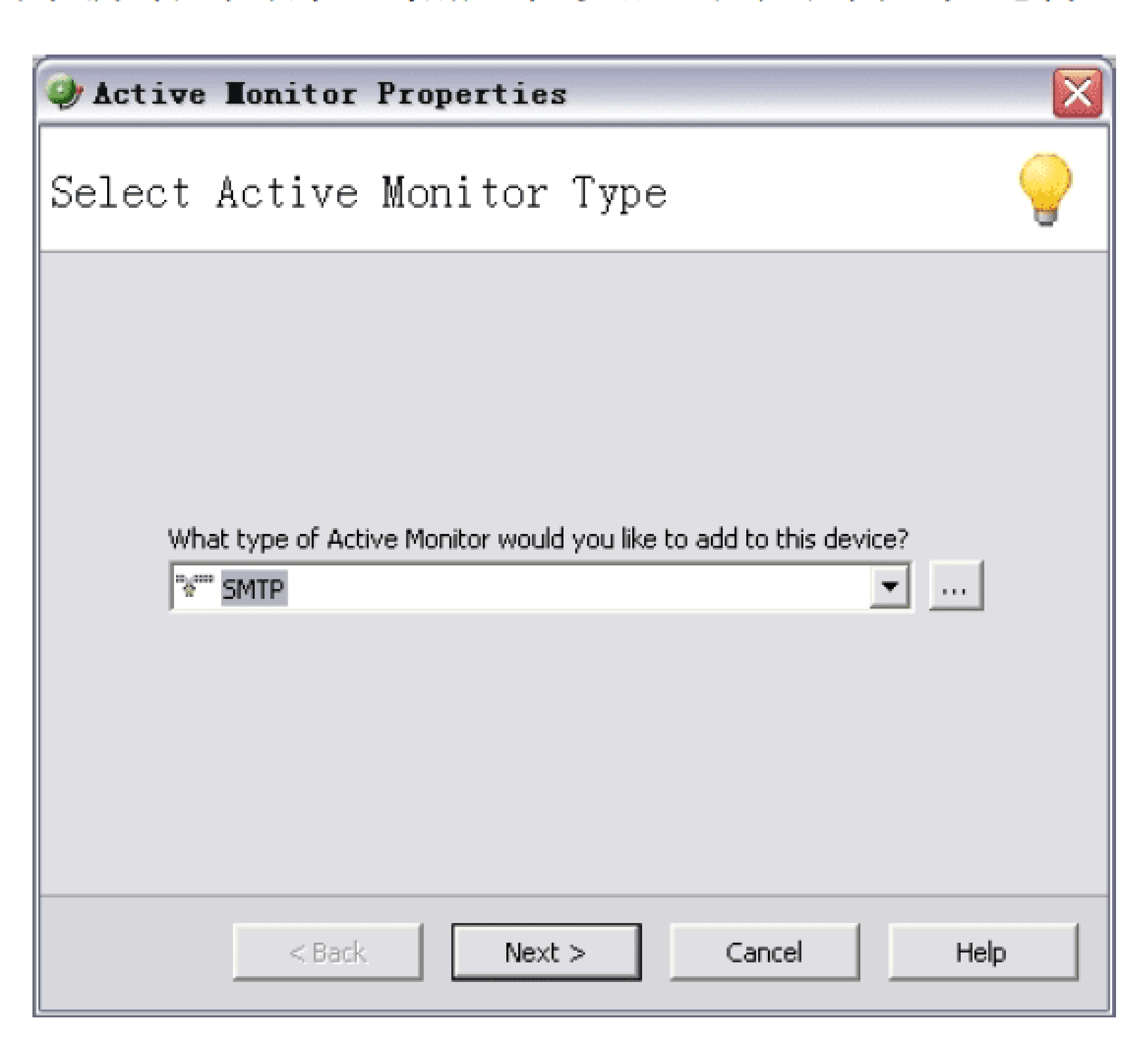


图 7-46　选择新建 SMTP 的监测项目

（3）进入下一步，为该监测项目添加报警提示动作即完成 SMTP 服务的监测。同样，可以为邮件服务器添加 POP3、IMAP4 和 DNS 服务等主动监测项目。

7.3.5 配置 Exchange 综合监测项目

除 SMTP、POP3 常规服务外，WhatsUp Gold 还提供了对 Exchange 其他服务的综合监测，包括监测硬件性能、系统参数阈值及 Exchange 服务的后台进程状态等多项内容。只要对象中其中一项超过阈值，则该 Exchange 综合监测项目就会发出报警提示。建立步骤如下：

（1）在 WhatsUp Gold 主界面的配置菜单中选择主动监测库 Active Monitor Library，单击 New 按钮，并从活动监测类型下拉列表中选择 Exchange 监测 Exchange Monitor，如图 7-47 所示。



图 7-47 选择新建监测的类型为 Exchange

（2）进入配置界面，在 Name 文本框中输入自定义项目名称。在 Threshold to monitor 列表框中列出了可监测的参数及其阈值设定，选择需要监测的对象，并可根据需要修改其阈值。在 Services to monitor 列表框中列出了可监测的 Exchange 服务对象，可根据需要选择监测服务，如图 7-48 所示。

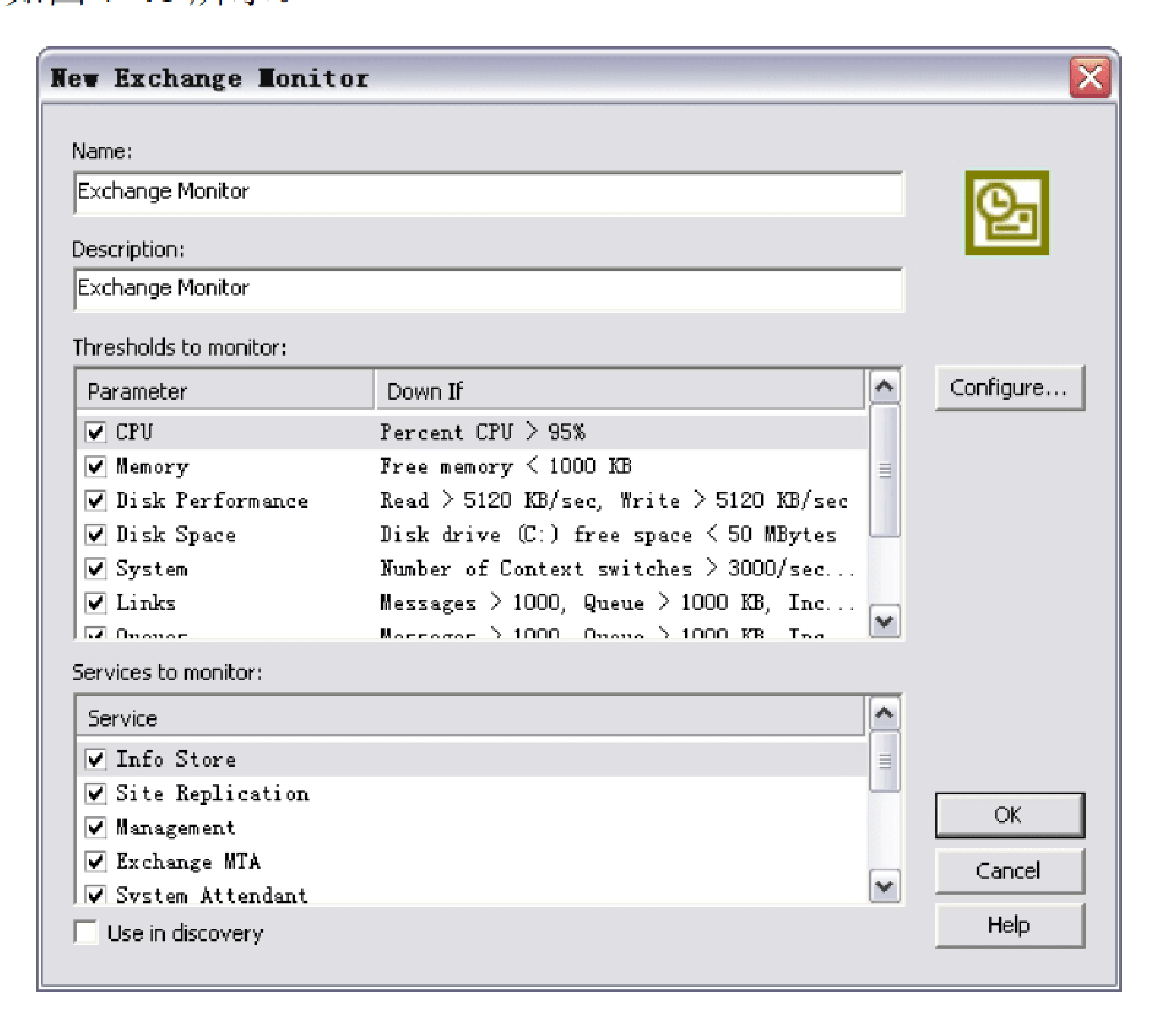


图 7-48 配置 Exchange 监测参数和服务对象

（3）在参数监测中（如 CPU 参数）双击该选项或单击 Configure 按钮，在弹出的对话框中可输入 CPU 使用率报警阈值。在 CPU 使用率超过默认阈值 95%时，将发出报警提示。该参数可根据实际需要进行修改。其他设置项目还包括邮件所占磁盘容量的阈值（如图 7-49 所示）、未使用的内存容量、磁盘存取速度、磁盘空间等，这些参数的设置较为直观。

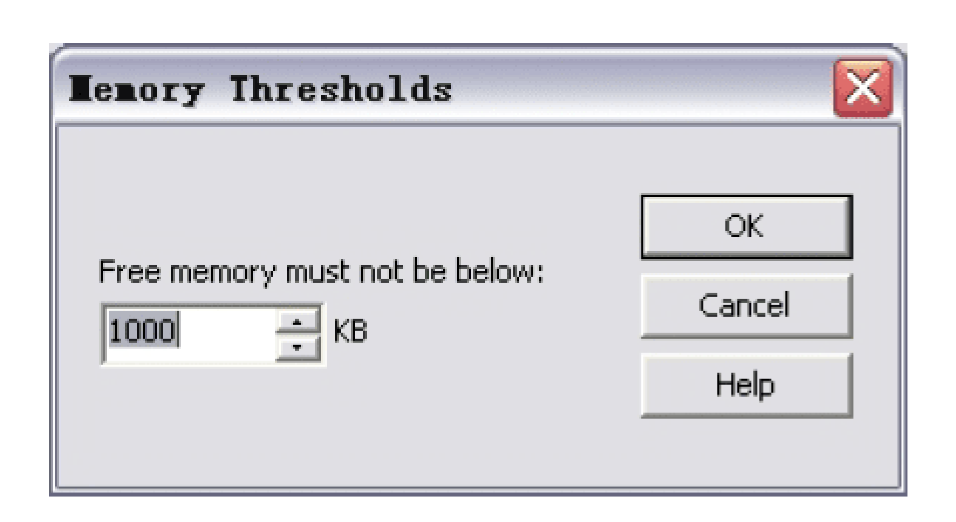


图 7-49　修改邮件所占容量的报警阈值

（4）配置结束后返回到主动监测库界面，对新建的 Exchange Monitor 监测选项进行测试。单击 Test 按钮，进入测试对象选择对话框。在对话框中需要选择包含 Exchange 服务的主机对象，以及选择访问目标主机的 Windows 凭证，然后单击 Test 按钮进行测试。如果返回信息提示服务正常，说明该监测对象设置正确，如图 7-50 所示。

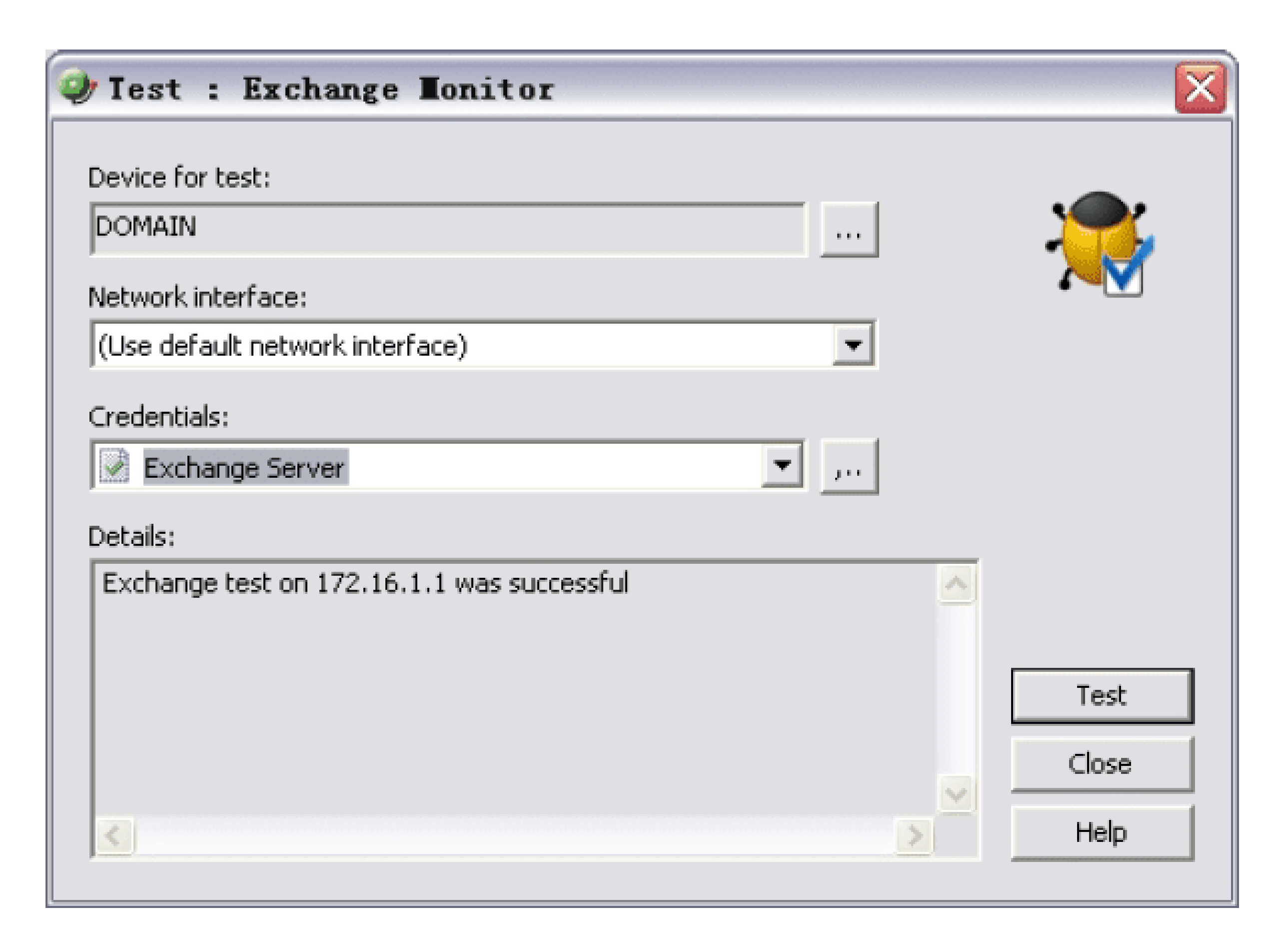


图 7-50　测试新建的邮件监测项目

（5）查看 Exchange 服务器监测结果。进入 Web 视图，并选择该设备的报表界面。该界面的 Device Active Monitor States 面板中列出了所有的主动监测对象状态，如图 7-51 所示。

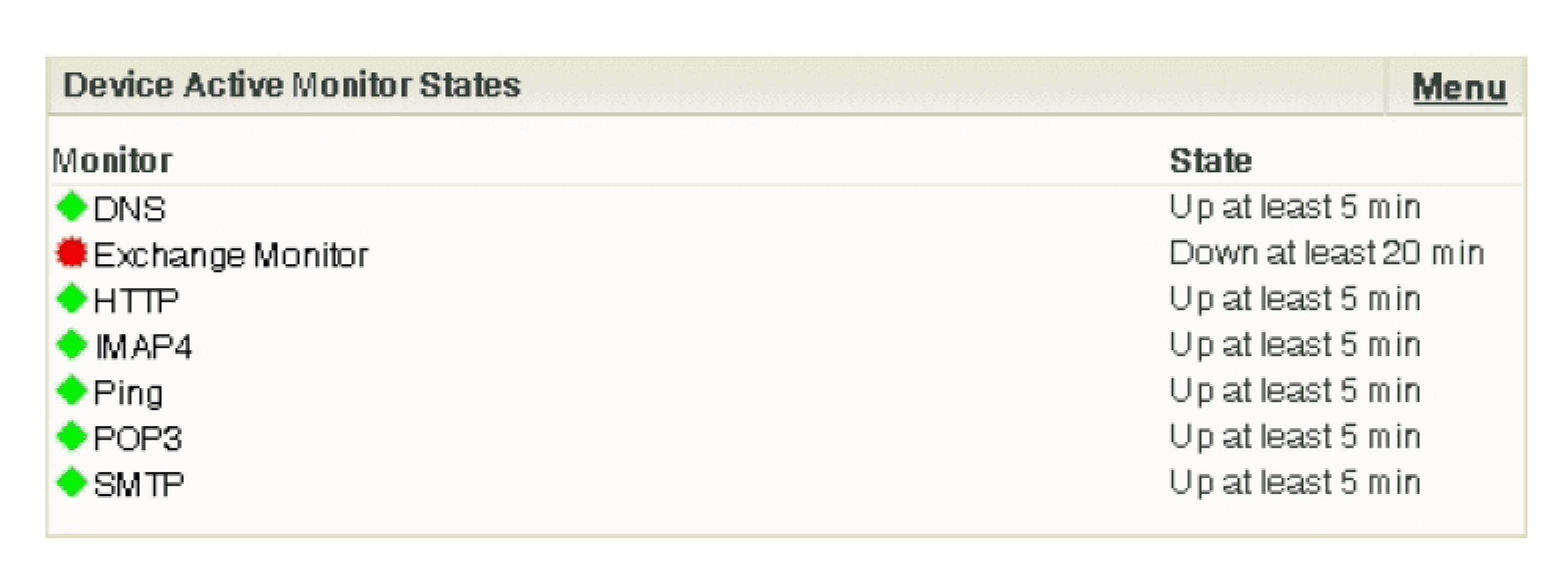


图 7-51　在 Web 界面中查看监测对象的状态

选择查看 SMTP 的历史信息，如图 7-52 所示。

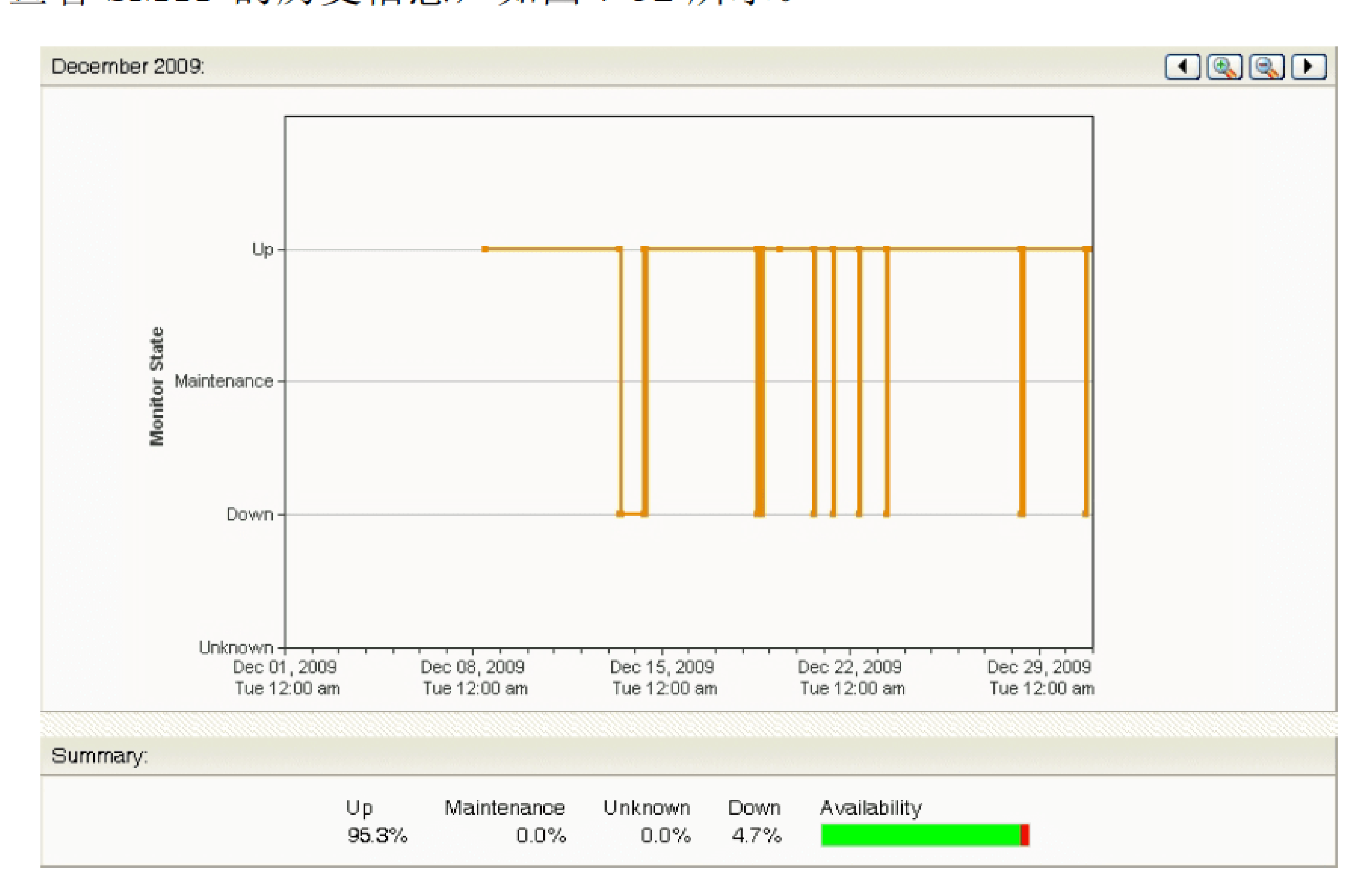


图 7-52　选择查看 SMTP 监测的历史信息

在图 7-52 中可看到 2009 年 12 月 18 日发生服务停止的时间较长，选择 18 日区域，就可放大图像，了解具体的故障时段，如图 7-53 所示。

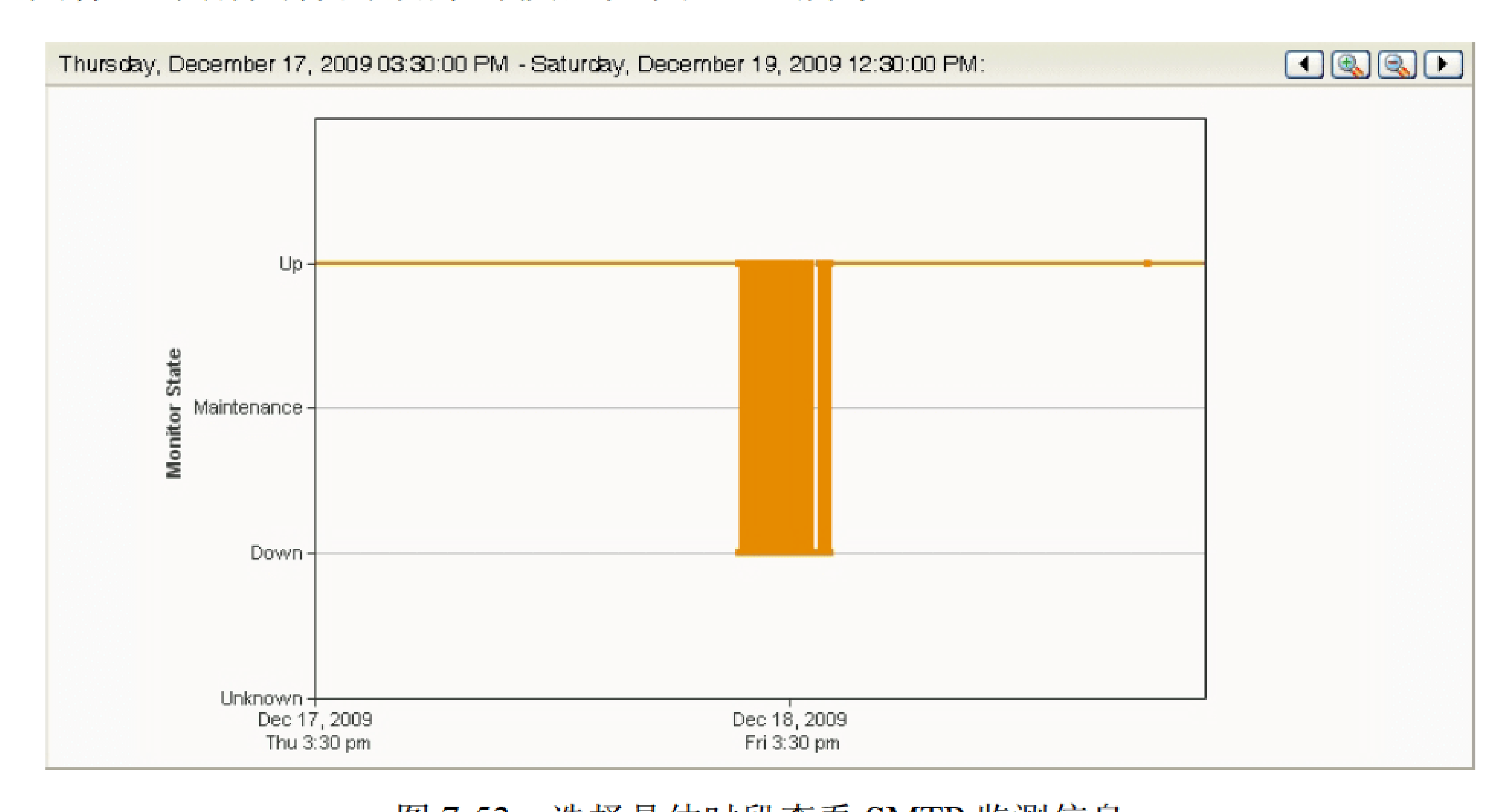


图 7-53　选择具体时段查看 SMTP 监测信息

此时可对比 Ping 的服务历史记录，可以看到 Ping 服务的监测结果报表与 SMTP 监测的图形一致。那么可以判断 SMTP 服务的失败是由于 Ping 不通，所以采集不到数据而触发报警。当然也可能由其他原因造成，可根据邮件服务器的日志记录等方式进行检查。

7.4 Passive Monitors 被动监测

被动监测类型共包括 3 类：SNMP Trap（Trap 消息）、Syslog（监测系统日志）、Windows

Event Log（监测 Windows 事件日志）。以下分别对 3 种类型进行介绍。

7.4.1 实例 1：添加 SNMP Trap 被动监测

在第 1 章中介绍了 Trap 消息的原理，包括被监测对象发送 Trap 和网管主机接收 Trap 的机制。要通过 WhatsUp Gold 监测 Trap 消息，首先需要在被监测对象中开启 Trap 允许，以及设置接收 Trap 消息的主机，然后在 WhatsUp Gold 中添加 Passive Monitors（被动监测）项目。添加步骤如下：

（1）在设备属性 Passive Monitors 对话框中，单击 New 按钮，并在被动监测类型下拉列表中选择 SNMP Trap，对象选择 Any，即监测所有的 Trap 消息，如图 7-54 所示。

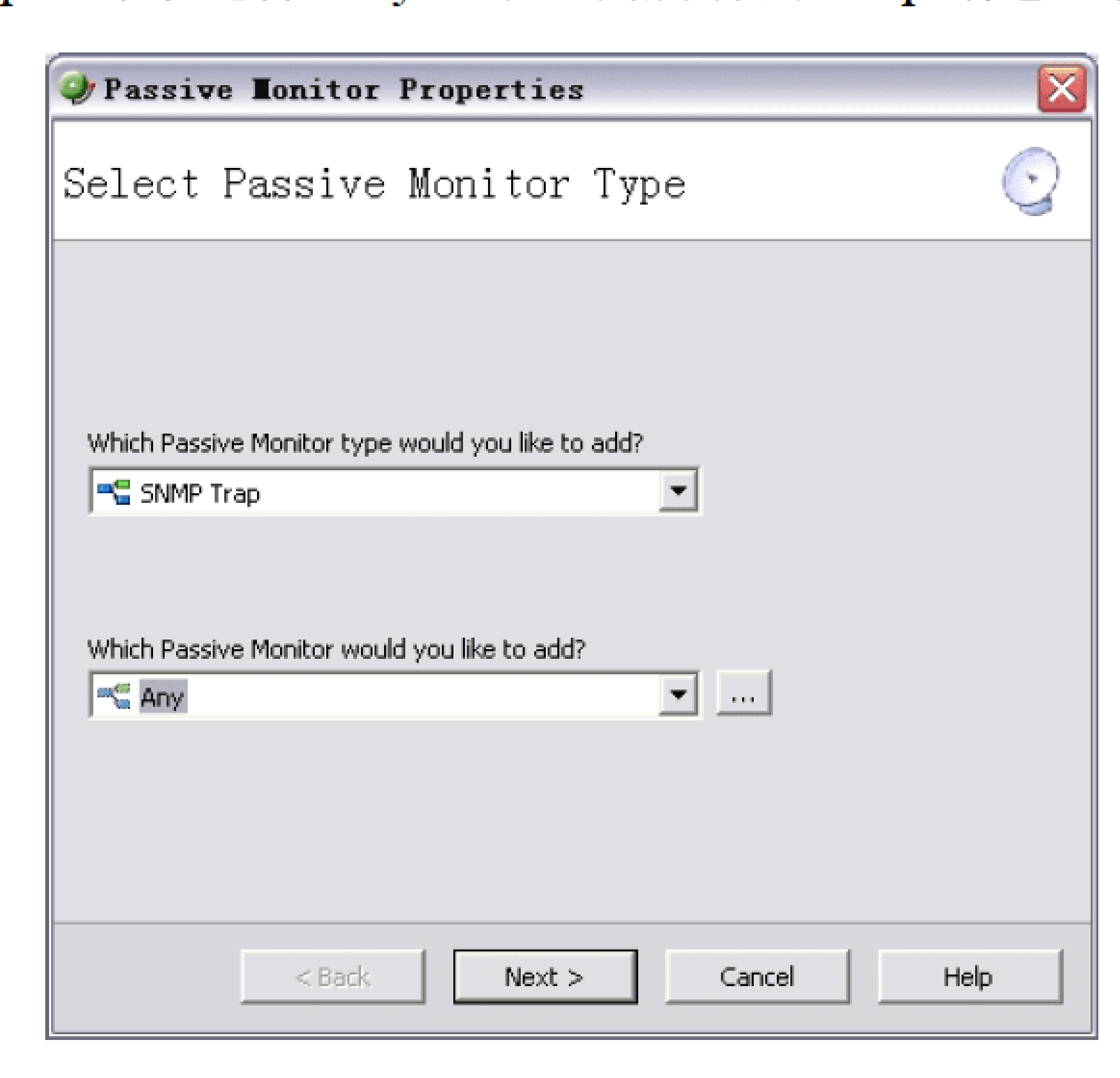


图 7-54 新建 Link Down 的被动监测项目

（2）单击 Next 按钮进入下一步，为该监测项目添加报警提示动作，如图 7-55 所示。

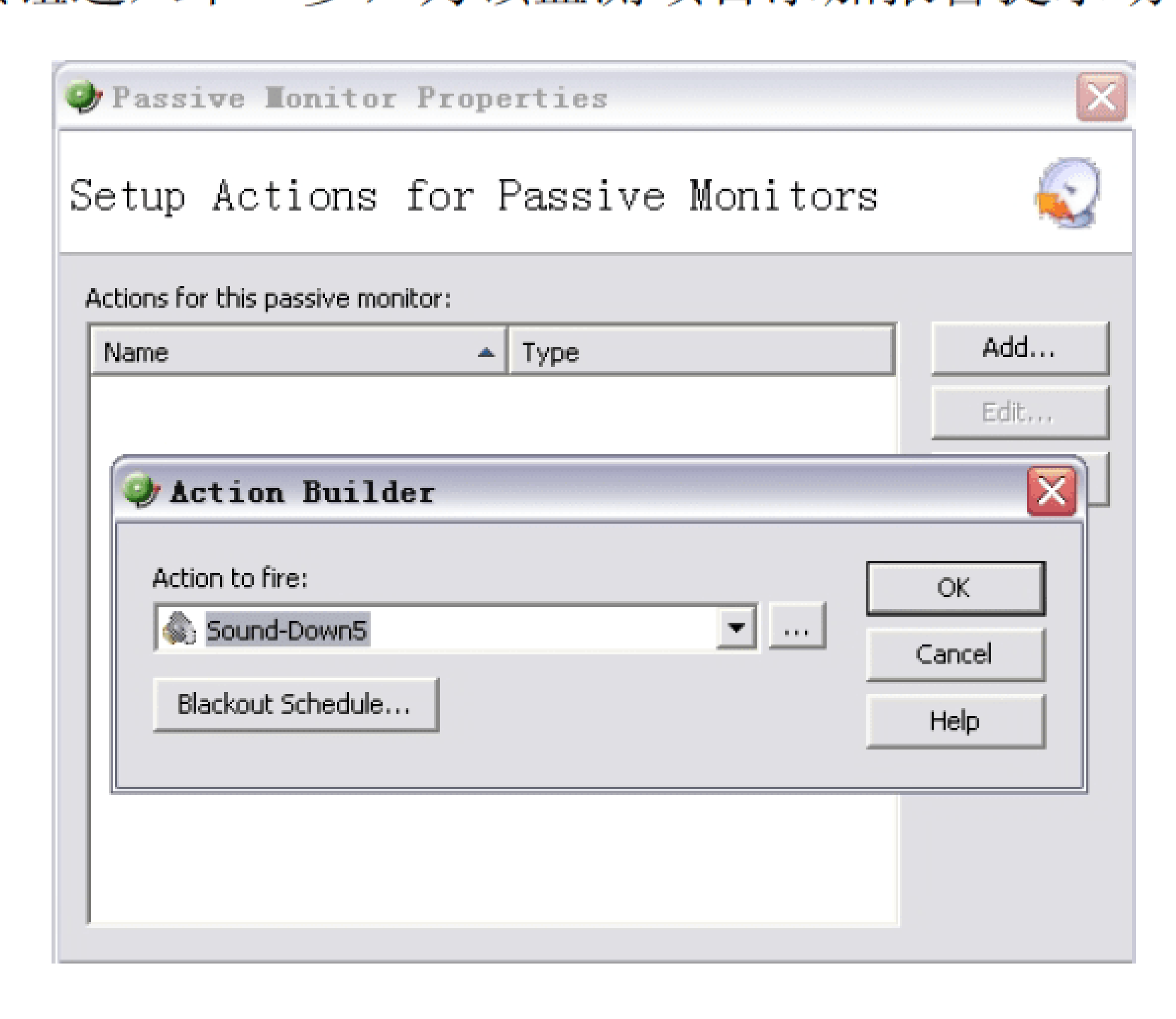


图 7-55 为被动监测项目添加报警动作

（3）添加完成后，该被动监测项目出现在 Passive Monitors 页面的列表中，如图 7-56 所示。

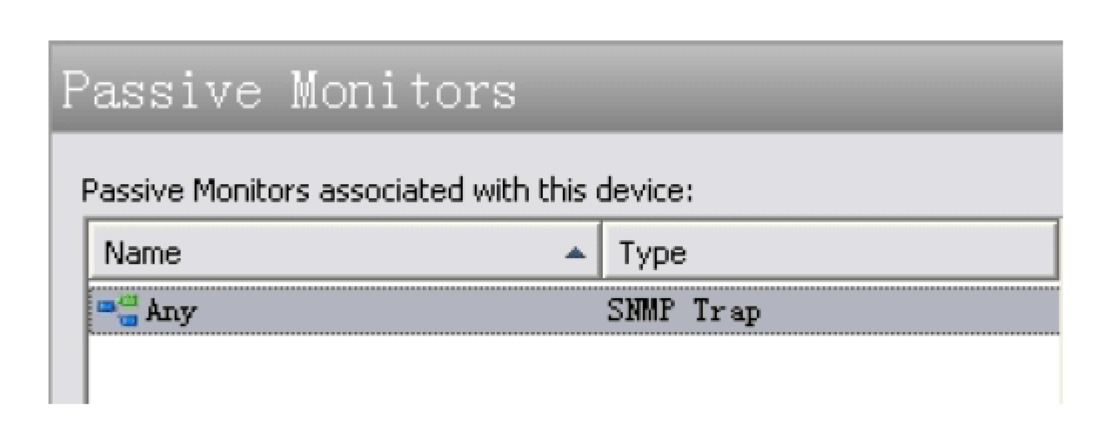


图 7-56　被动监测项目列表

（4）在添加完成后，待收集到一定数量的 Trap 消息后可通过 Web 进行查看。收到的信息列表如图 7-57 所示。

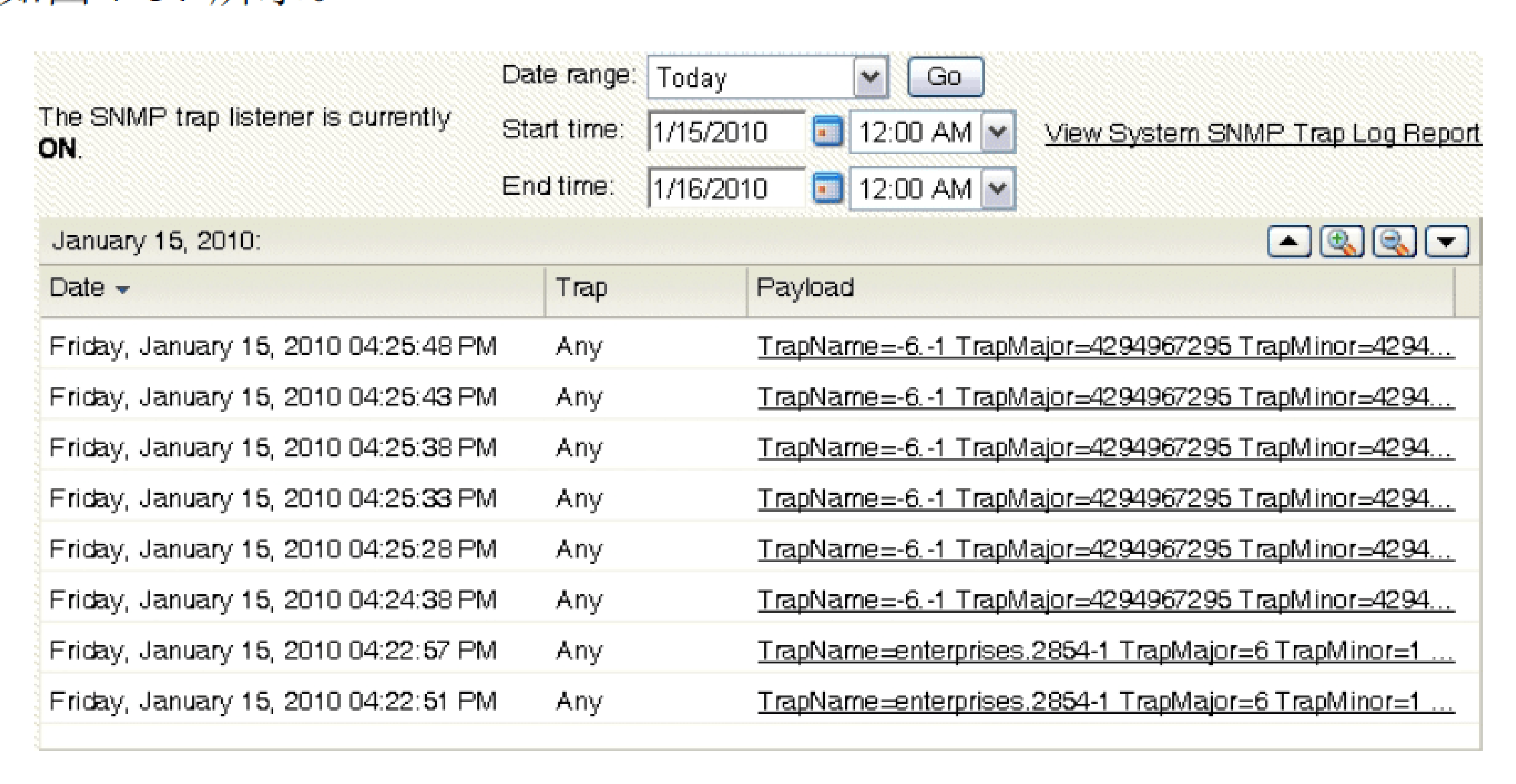


图 7-57　在 Web 界面查看收到的 Trap 信息

单击一条记录即可查看 Trap 信息的具体内容，包括信息类型、社区字符串、OBI 等信息，如图 7-58 所示。

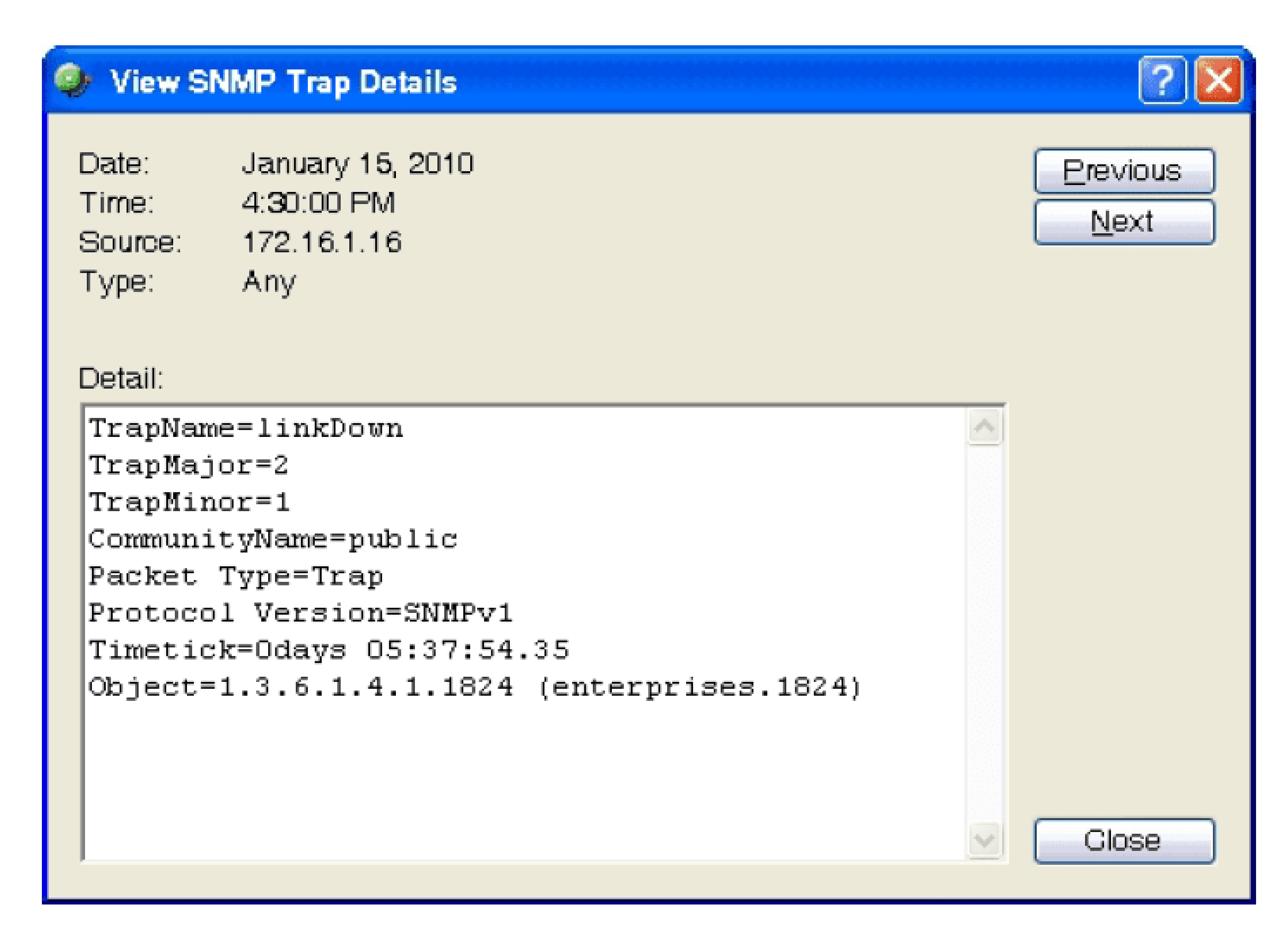


图 7-58　Trap 信息内容

7.4.2 实例 2：添加 Syslog 被动监测

添加一个 Syslog 被动监测项目，对系统日志中包含 DNS（域名）字样的日志内容进行监测。只要系统产生了与 DNS 相关的日志，则发送信息至网管程序并触发报警提示。添加步骤如下：

（1）选择主界面的 Configure | Passive Monitor Library 菜单命令，打开被动监测项目库，在列表中列出了所有可为设备添加的被动监测项目。单击 New 按钮弹出新建对话框，并在项目类型下拉列表中选择 Syslog，如图 7-59 所示。

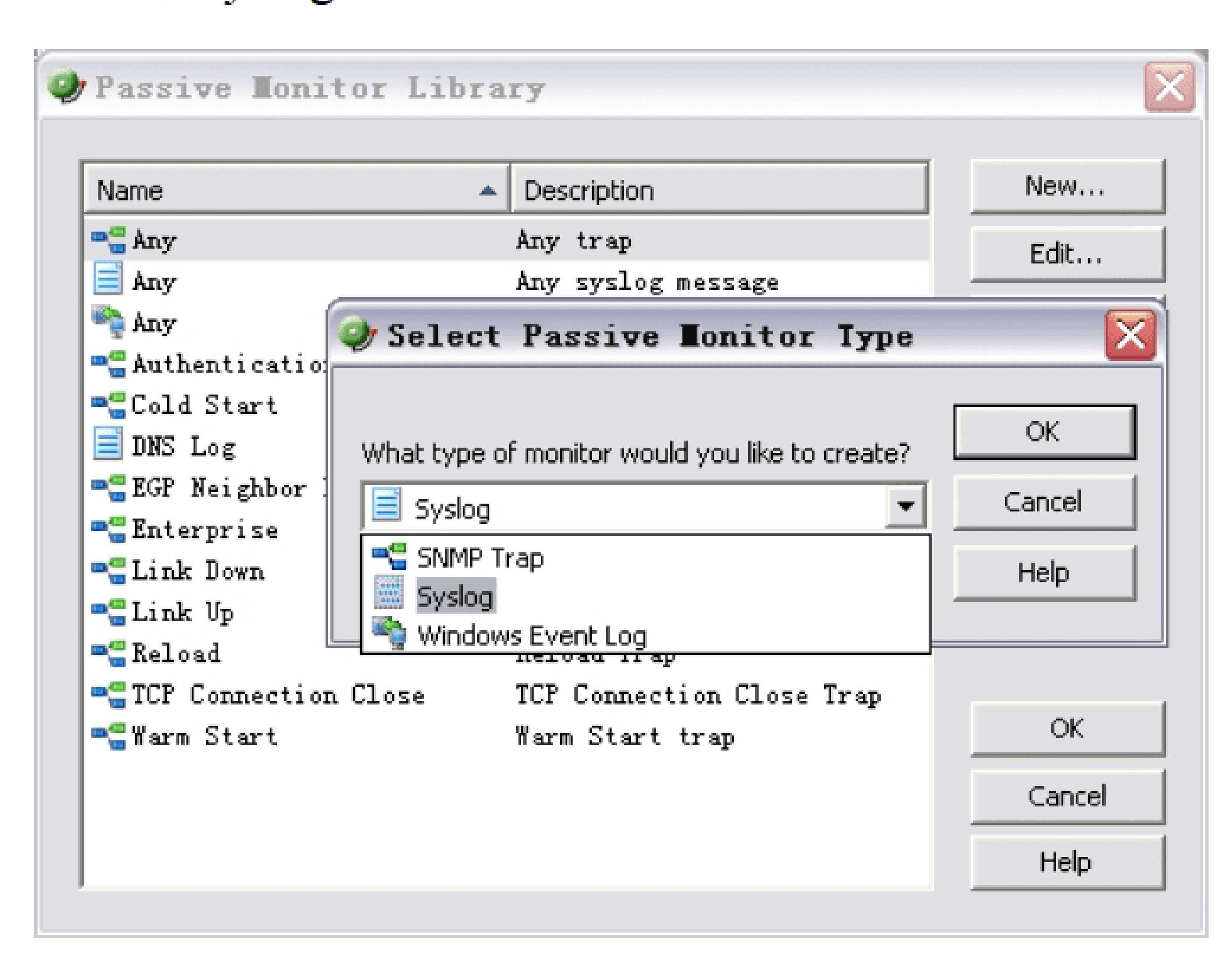


图 7-59　新建系统日志被动监测

（2）单击 OK 按钮进入规则设置对话框。在表达式 Expression 文本框中输入要监测的日志内容摘要。此处对包含 DNS 的日志进行监测，那么输入 DNS 确认后，就完成了添加步骤，如图 7-60 所示。

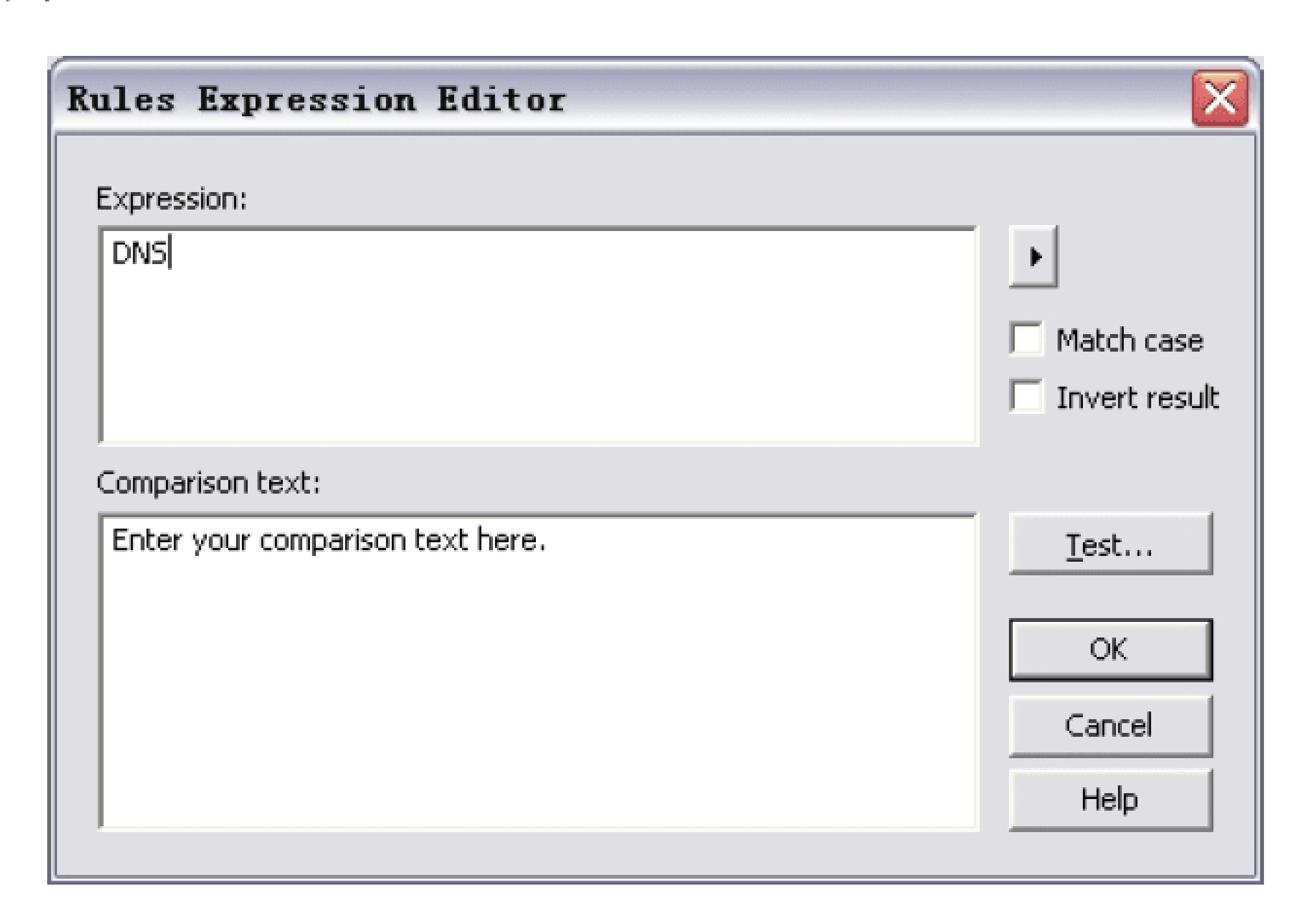


图 7-60　新建系统日志被动监测

（3）新建该被动监测项目后，并未应用到具体设备上，还需在提供的 DNS 服务的主机对象中添加该被动监测项目。

7.4.3 实例 3：添加 Windows Event log 被动监测

添加一个被动监测项目对操作系统中的事件日志进行监测，只要系统产生了事件日志或指定的事件日志，则通知网管程序并触发报警提示动作。其添加过程类似于新建系统日志监测项目，步骤如下：

（1）进入被动监测项目库，并单击 New 按钮弹出新建对话框，在类型下拉列表中选择 Windows Event Log，如图 7-61 所示。

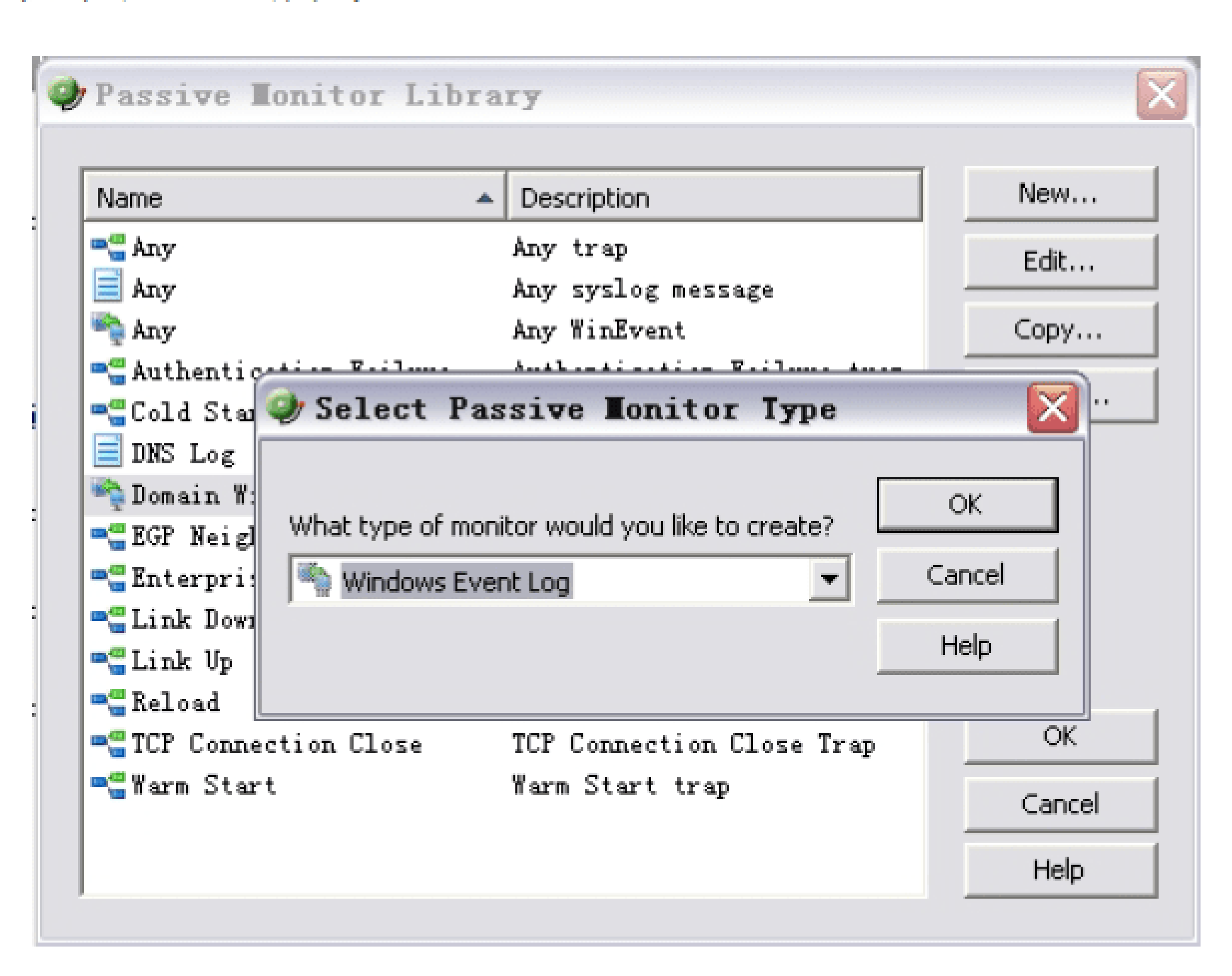


图 7-61 新建 Windows Event Log 的被动监测

（2）单击 OK 按钮进入设置对话框。在 Name 文本框中输入该项目的名称。在 Provide an account that has administrative rights 文本框中输入目标主机的账户名和密码，该账户需要具备管理员权限。在 Condition（条件）文本框中可设置过滤条件，如果不添加任何过滤条件，则对所有生成的事件日志进行监测，如图 7-62 所示。

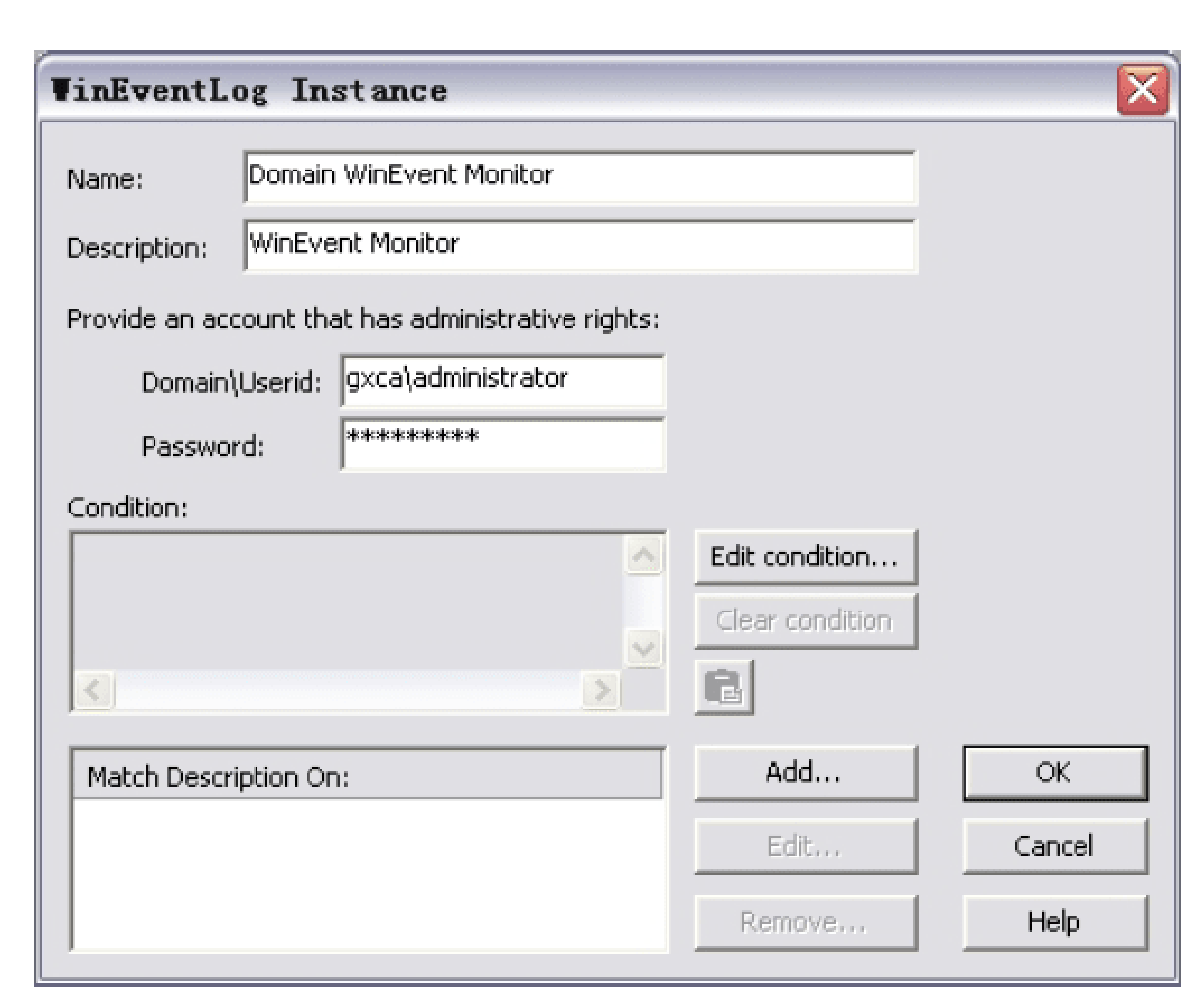


图 7-62 设置事件日志进行监测

（3）在新建该被动监测对象后，还需将该监测添加到被监测设备中。

经过以上实例的介绍，即完成了在 WhatsUp Gold 程序中采集信息、添加配置性能监测、添加配置主动监测和被动监测。网管员可通过多执行操作来熟悉这些监测项目的配置和应用。

7.5 配置 WhatsUp Gold 多监视器网管结构

由于 WhatsUp Gold 提供了控制台视图、拓扑视图、Web 视图及报表视图等，所以网络管理员需要查看的监测内容也非常多。那么仅使用一台显示器查看 WhatsUp Gold 监测信息的效率并不高。本节介绍安装和配置 WhatsUp Gold 同时使用多个显示器监测网络状态，使得网管员在同一时间能查看更多的网络信息。

方式很简单，只需要在一台 WhatUp Gold 的主机中通过增加一块双输出显卡和另外一台显示器，就能够构建一个多监视器的展示界面，如图 7-63 所示。

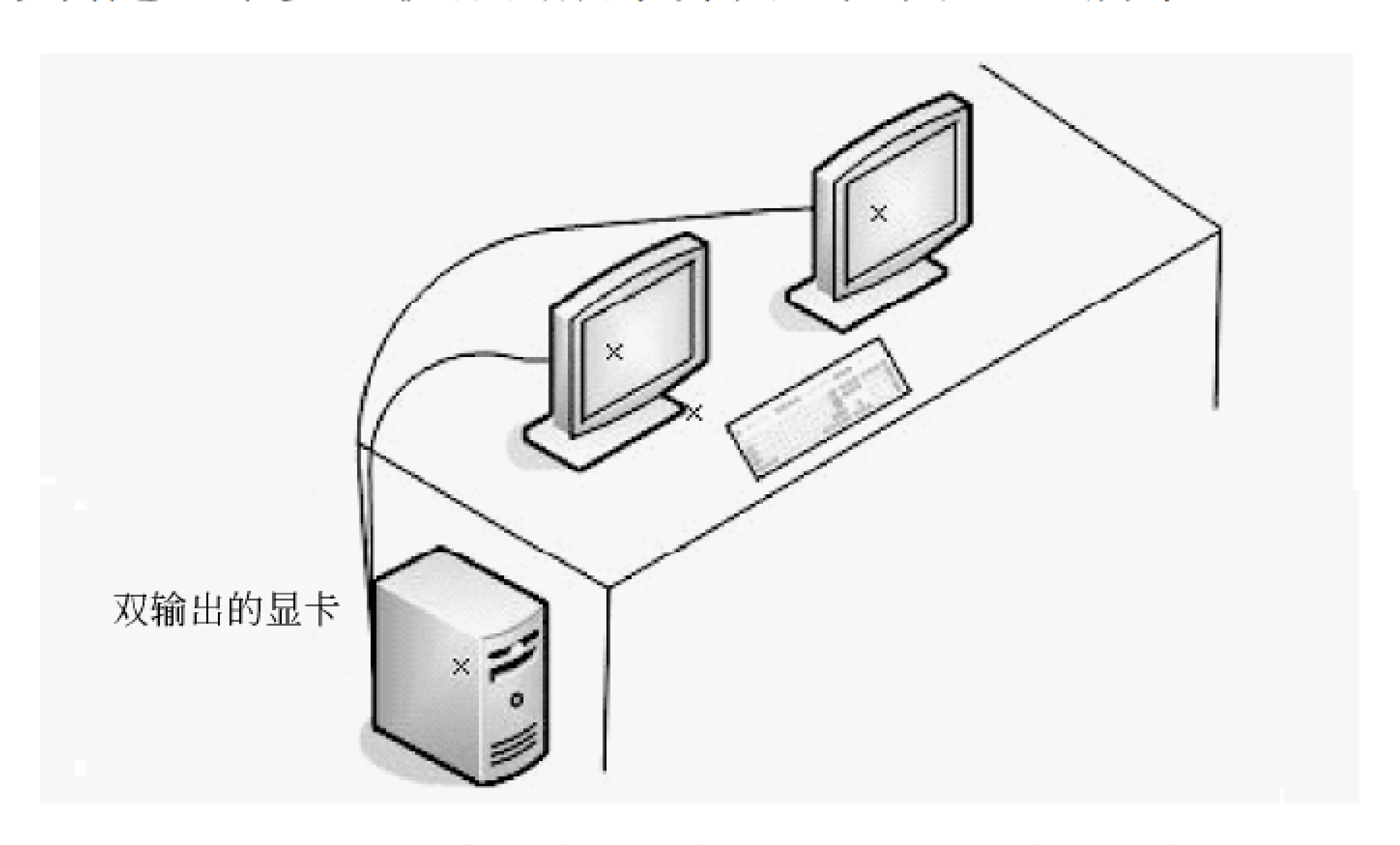


图 7-63　通过双输出显卡配置多显示器监测网络

注意：如果需要增加更多的显示器，那么可以在安装了 WhatUp Gold 的操作系统中安装两块有双显示输出接口（一块显卡上有两个输出接口）的显卡，则可将显示内容扩展到 4 个显示器上。

以下介绍双输出显卡的配置。通过配置可以使用同一块显卡连接的两个显示器中展示不同内容。本例以 ATI Radeon HD4670 型号的显卡为示例，如图 7-64 所示。

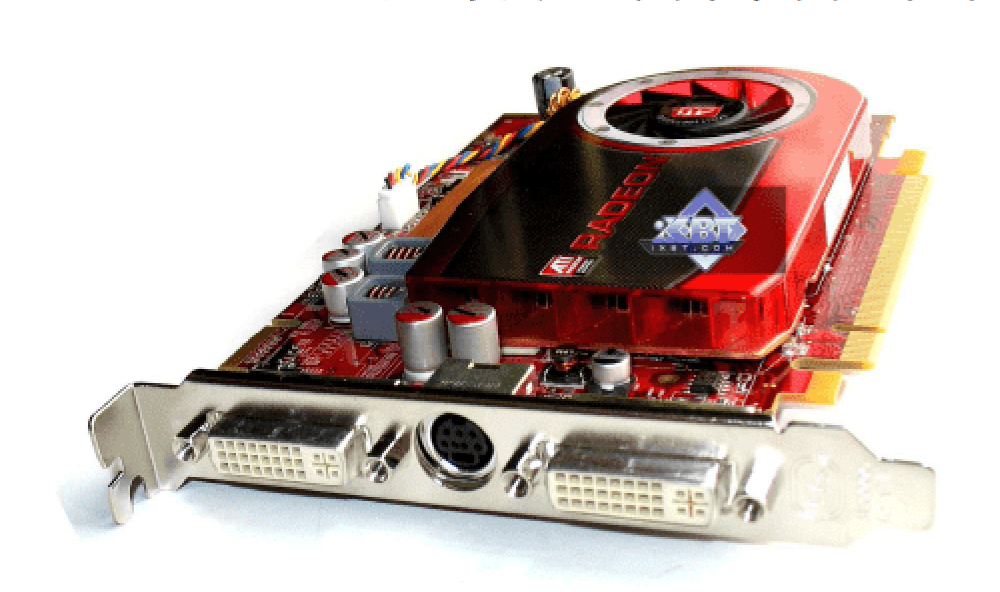


图 7-64　带双输出接口的 ATI 显卡

配置步骤如下：

（1）该显卡使用的是 DVI 模式输出接口，还需要通过转接头将其转换为 VGA 输出，并分别连接至两台显示器，在安装完硬件设备后，即可配置显卡输出。

（2）在 Windows 窗口中右击，打开右键菜单，选择【属性】|【显示】对话框，则在显示器配置选项卡中可以看到两个模拟显示器，分别对应了显卡的两个输出接口。选择监视器 2，并选中“将 Windows 桌面扩展到该监视器上”复选框，如图 7-65 所示。



图 7-65　打开显示属性设置界面

（3）单击【高级】按钮，进入显卡的高级选项设置界面，然后单击 Catalyst Control Center 按钮，以配置显卡的扩展显示属性，如图 7-66 所示。



图 7-66　显卡属性设置界面

（4）在显卡配置对话框中，可以看到该显卡已经发现了两个显示器，默认的将第一个显示器作为主显示器，如图 7-67 所示。



图 7-67　设置主显示器

（5）进入下一步，在显示方式界面中选择【水平拉伸】选项，即将原始桌面显示内容扩展到两个显示器中，如图 7-68 所示。

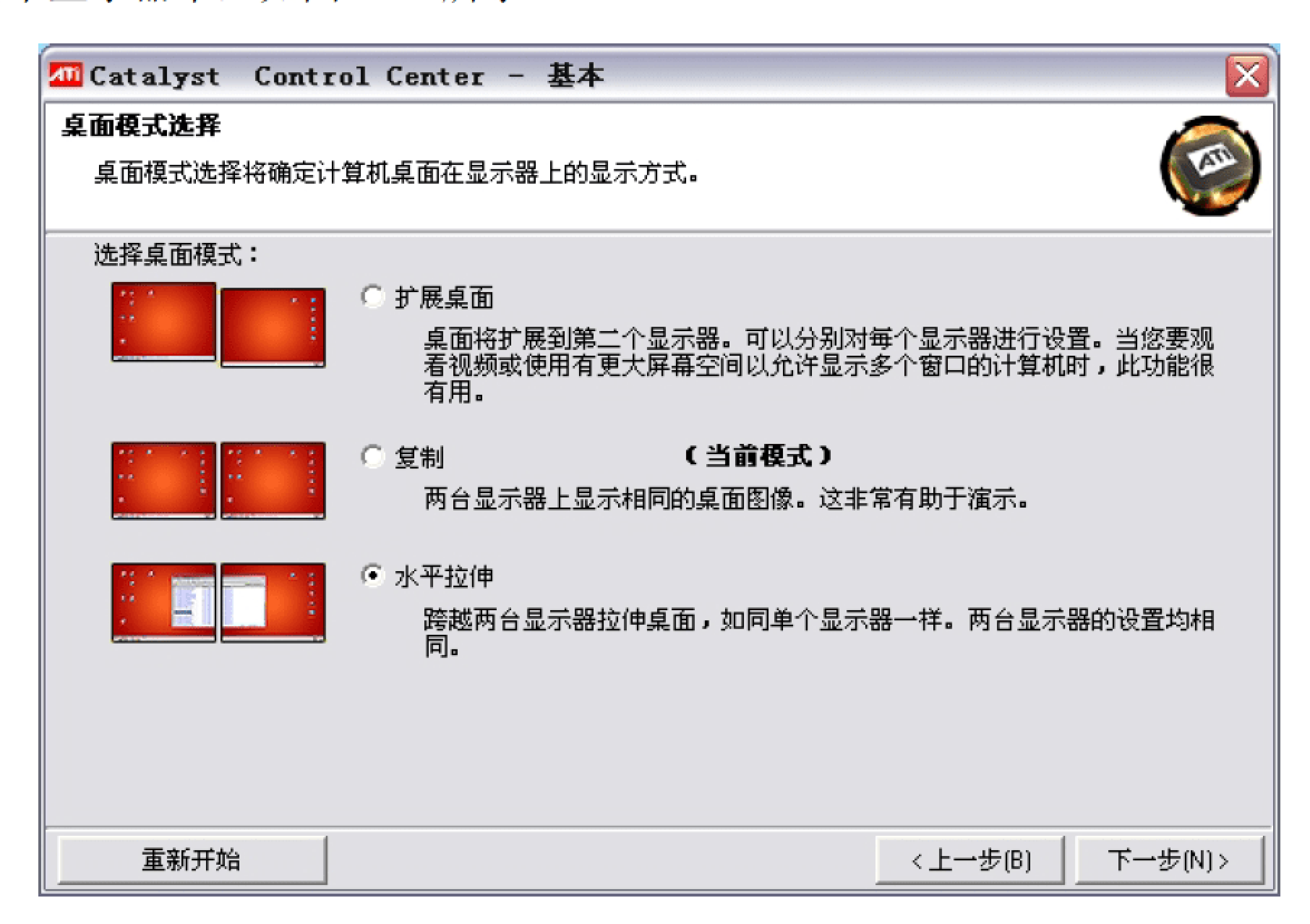


图 7-68　设置显卡扩展显示方式

（6）此时，Windows 窗口和鼠标操作都能够在两个显示器中进行穿越。回到 WhatsUp Gold 程序中，将其网页视图和 Windows 视图分别拖放到不同的显示器中即可。

7.6 本章小结

通过本章的实例学习，可以理解 WhatsUp Gold 不同类型的监测方式，并能够配置实现性能采集、设备对象监测、服务对象监测，以及对特种设备状态监测等。网络管理员可通过多操作，熟练使用 WhatsUp Gold 监测功能并获取需要的报表信息。

第 8 章　Web 界面及报表应用详解

在对 WhatsUp Gold 控制台功能进行实例讲解后，本章主要介绍 WhatsUp Gold 的 Web 模式，以及 Web 模式下报表的相关应用。通过对本章的学习，网管员应能够熟练应用 WhatsUp Gold 在 Web 界面的各项操作，能够根据自定义需要生成期望的报表信息。本章主要内容如下：

- 配置自定义的 Workspace 视图；
- Workspace 报表；
- 报表界面使用介绍。

8.1 Home 视图介绍

WhatsUp Gold 在 Web 模式中的 WorkSpace（工作间）是一个可通过需要来定制多显示区域的视图界面，这个视图通过报表、图表等方式展示用户各类数据信息。当需要创建自定义视图时，首先需要考虑什么是查看最频繁的信息及最关注的信息。还需要查看数据的详细程度，同时还需要考虑能加入到新工作间视图的报表类型。

登录到 WhatsUp Web 界面中并使用 admin/admin 账户登录，首先看到的就是 Home 工作间视图，该视图包含进入其他报表的链接、统计信息和帮助文档链接等综合信息，如图 8-1 所示。

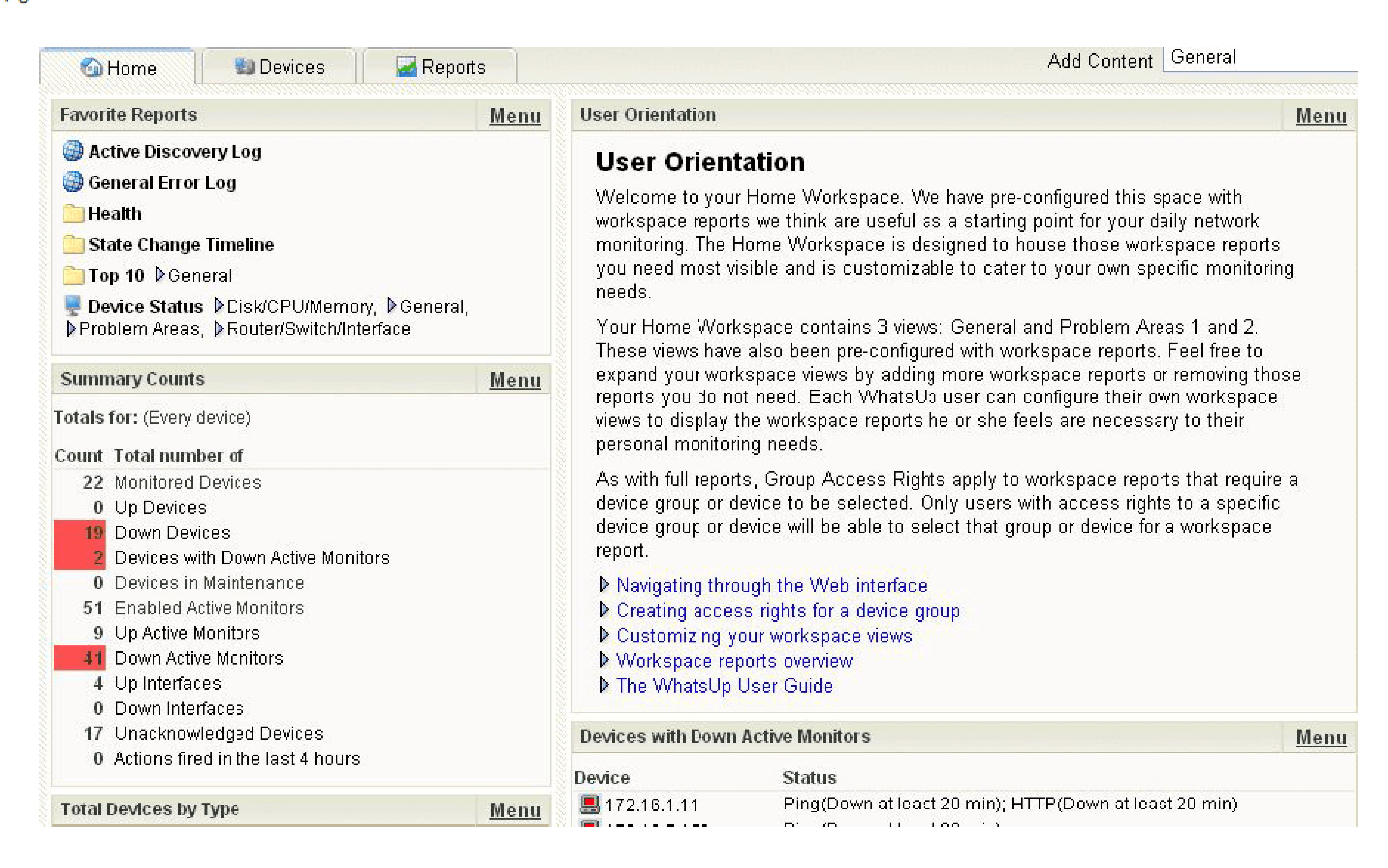


图 8-1　登录到 Web 界面视图

8.1.1 视图分类

在 WhatsUp Gold V11 Web 界面中提供了 3 种预设的 WorkSpace 视图类型。

- ❑ Home Workspace：包含各种整体统计信息的 Home 工作间视图。
- ❑ Device Status workspace：针对所选单一设备状态的信息视图。
- ❑ Top 10 workspace：按照各类状态进行排行，处于前十的信息视图。

这 3 种工作间视图，又各自包含不同侧重点的展示样式。这些样式是系统默认提供的，并可对其进行修改、删除，或者根据自己感兴趣的内容新建样式。3 种工作间视图默认包含的视图样式如图 8-2 所示。

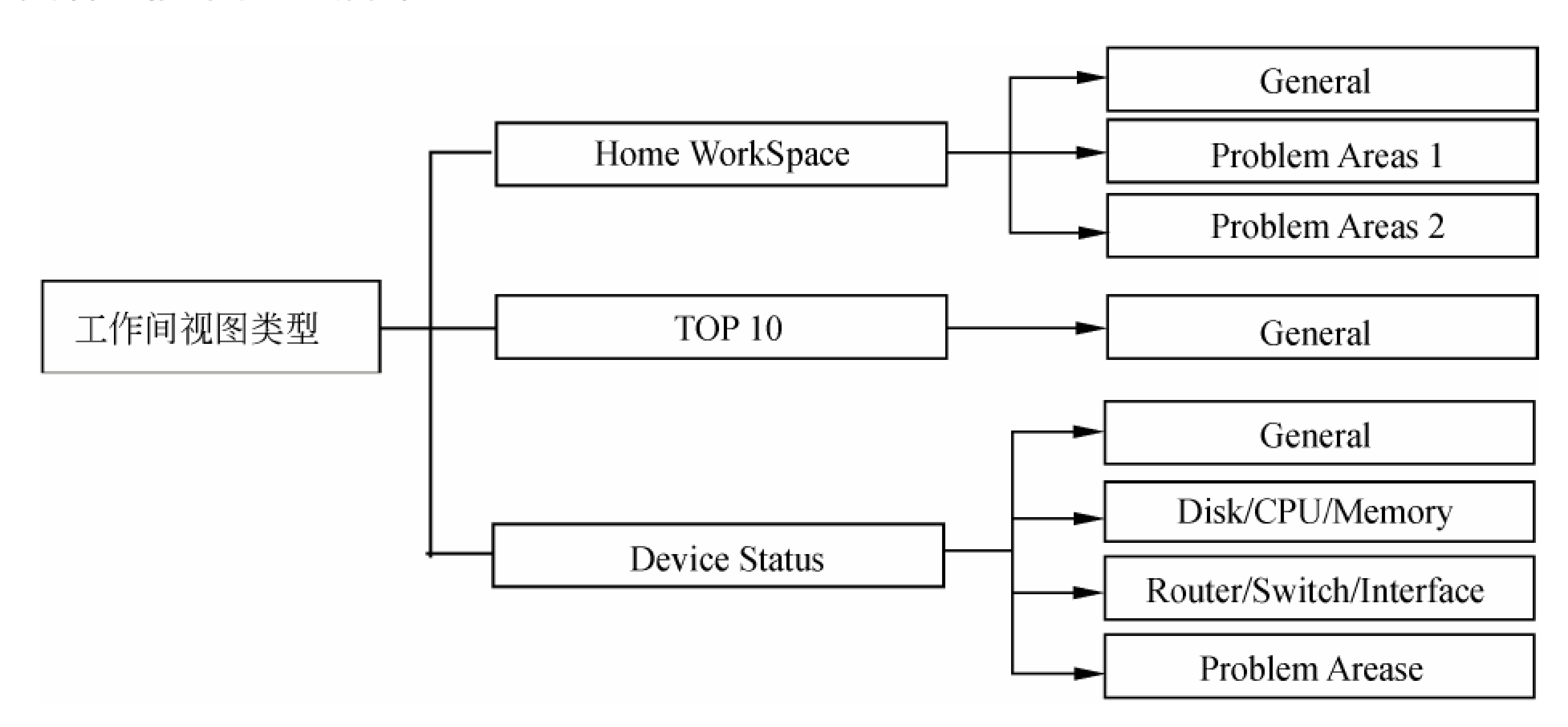


图 8-2　3 种类型 WorkSpace 各自包含的不同样式

在图 8-2 中，Home 工作间包含了 General（常规）和 Problem Areas（故障记录）的样式；Top 10 工作间默认只包含一种 General 显示样式；而 Device Status（设备状态）视图，可分为 General 样式、Disk/CPU/Memory（磁盘/CPU/内存展示）、Router/Switch/Interface（路由器/交换机/接口）和 Problem Areas 记录的 4 种样式，用户可以针对感兴趣的内容分别选择不同的样式进行有记录的查看。

以下分别介绍 3 类视图界面所展示的内容和应用。

8.1.2 Home 视图

Home WorkSpace 视图，可把这个界面看成一个“家”，也就是一个包含了其他报表信息和统计信息，而组合成了一间完整展示信息的家，它可直观地展示最需要了解的网路信息。进入 Web 界面，默认展开的就是 Home WorkSpace 视图，如图 8-3 所示。

在 Home 工作间中，提供了 3 种类型的展示结构，可通过配置来更改其显示内容。

- ❑ General：常规样式，包含了各种统计数据图表。
- ❑ Problem Areas 1：故障区域 1，仅显示存在报警的设备信息。
- ❑ Problem Areas 2：故障区域 2，显示存在报警设备的其他附加信息。

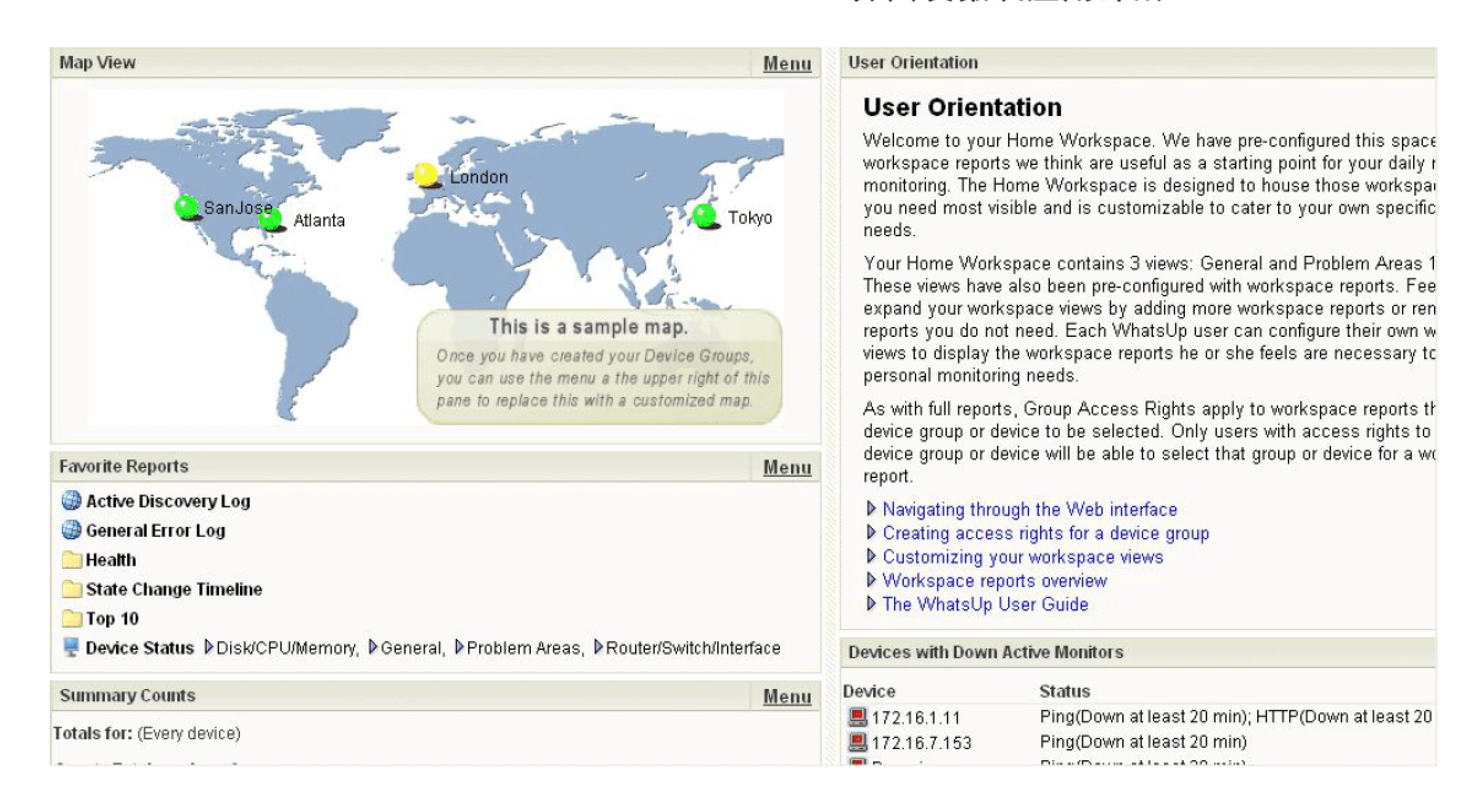


图 8-3　Home 工作间视图

可通过 Home 工作间右上角的按钮打开下拉列表，切换到不同的展示结构，如图 8-4 所示。

以下分别介绍这 3 种类型的报表结构。首先对 General 视图中包含的数据面板介绍如下。

在 General 视图中的 Favorite Reports 面板中列出了一些最常用的报表信息、设备硬件参数信息及 Top 10 排名信息等。值得注意的是 Health 信息，即查看所有设备及其监测项目的健康状态。

在 Summary Counts 面板中，列出了不同状态的设备数量合计和监测项目的合计信息，这些统计数据能够让网管员实时了解网络整体故障统计情况，如图 8-5 所示。

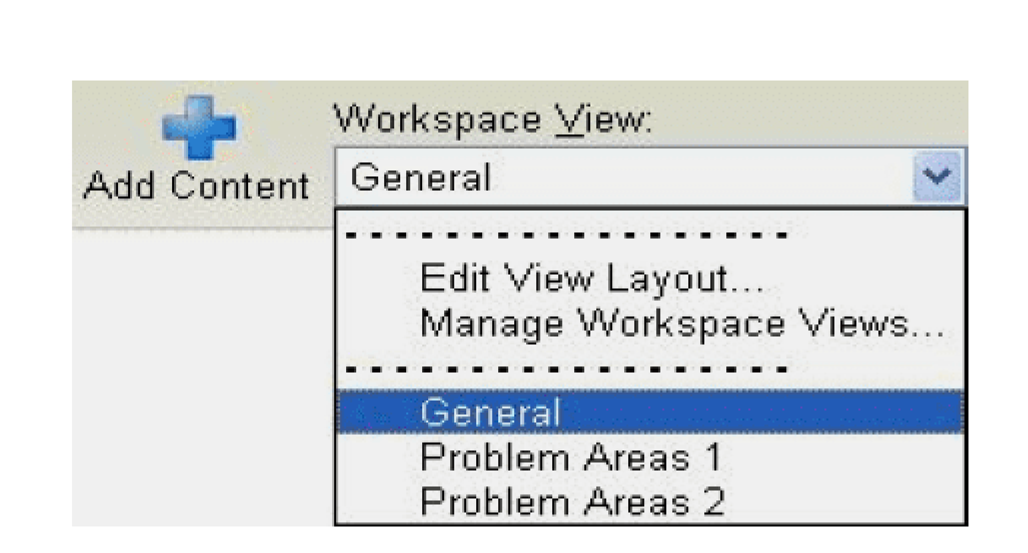


图 8-4　切换到不同的结构视图



图 8-5　各状态设备和监测项目统计

图 8-5 中提供了如下设备和监测项目的统计信息：

- ❑ 监视的设备；
- ❑ 状态为开启的设备；
- ❑ 状态为关闭的设备；
- ❑ 设备中包含停止的主动监测项目；
- ❑ 在维护中的设备；
- ❑ 主动监测项目；
- ❑ 状态为停止的主动监测项目；
- ❑ 状态为开启的端口；
- ❑ 状态为关闭的端口；
- ❑ 最近 4 小时设备状态变化引起的报警。

通过选择响应统计数据，能够查看统计项的细目信息。

在 Total Devices by Type 面板中按照设备类型对设备进行了统计，如图 8-6 所示。

Total Devices by Type		Menu
Device Type	Percentage	Count
Workstation	63.6%	14
Web Server	13.6%	3
HP Printer	9.1%	2
Windows Workstation	9.1%	2
Mail Server	4.5%	1

图 8-6　按照设备类型统计

介绍完常规样式后，介绍 Problem Area 故障区域样式。在故障视图中包含了设备或监测对象状态变化日志、报警动作执行日志、完全停止的设备列表等信息，通过该视图能够一目了然地看到网络中存在的问题，如图 8-7 所示。

Tail of State Change Log			Menu
Start time	Device	Monitor	State
Sun 11/08 8:45 PM	Domain	HTTP	Up at least 5 min
Sun 11/08 8:44 PM	Domain	Interface (3) - Intel(R) 825...	Up at least 5 min
Sun 11/08 8:44 PM	Domain	Interface (131077) - WAN ...	Up at least 5 min
Sun 11/08 8:43 PM	localhost	Interface (131077) - WAN ...	Up at least 5 min
Sun 11/08 8:43 PM	localhost	Interface (3) - Intel(R) 825...	Up at least 5 min

图 8-7　设备或监测项目状态变化日志

在 Problem Areas 视图中，列出了设备及监测项目。直接选择列表选项，即可进入单个设备的视图界面。在界面中，列出了所选设备的硬件利用率、主动监测项目状态、设备的 SNMP 属性及设备状态变化日志等信息。

Problem Areas 2（故障区域 2）与 Areas 1 视图类似，均为关注设备或监测项目发生的

故障日志。但在 Problem Area 2 中，更侧重于被动监测项目的故障日志，例如被动监测错误日志、SNMP 陷井日志、Syslog、Event log 等信息。

Home Workspace 能够展示整体的统计信息，同时还能显示针对单个设备的报表信息，是 WhatsUp Gold Web 模式中常用的视图界面。

8.1.3 Device Status 视图

在 Home Workspace 界面中，通过点击 Favorite Reports 面板中的 Device Status 链接，打开设备状态视图，如图 8-8 所示。

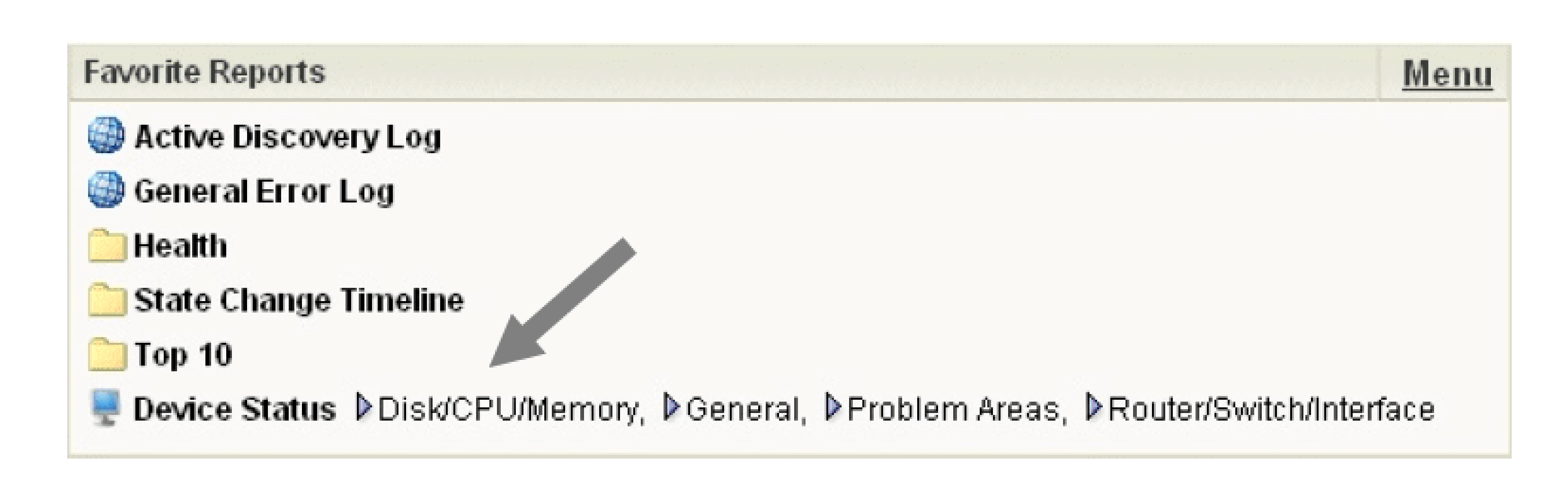


图 8-8　进入设备状态视图

在该视图中，首先打开的是该设备的常规信息界面。设备状态工作视图同样也提供了几种预先设定的结构视图，包括如下 4 种。

- ❑ General：常用信息图表，显示所选设备的综合信息。
- ❑ Disk/CPU/Memory：仅显示磁盘/CPU/内存使用率等信息。
- ❑ Problem Areas：故障区域，仅显示该设备有报警的信息。
- ❑ Route/Switch/Interface：仅显示路由器/交换机/接口信息。

同样，在该视图右上角的 View 下拉列表中可切换到不同的展示结构，如图 8-9 所示。

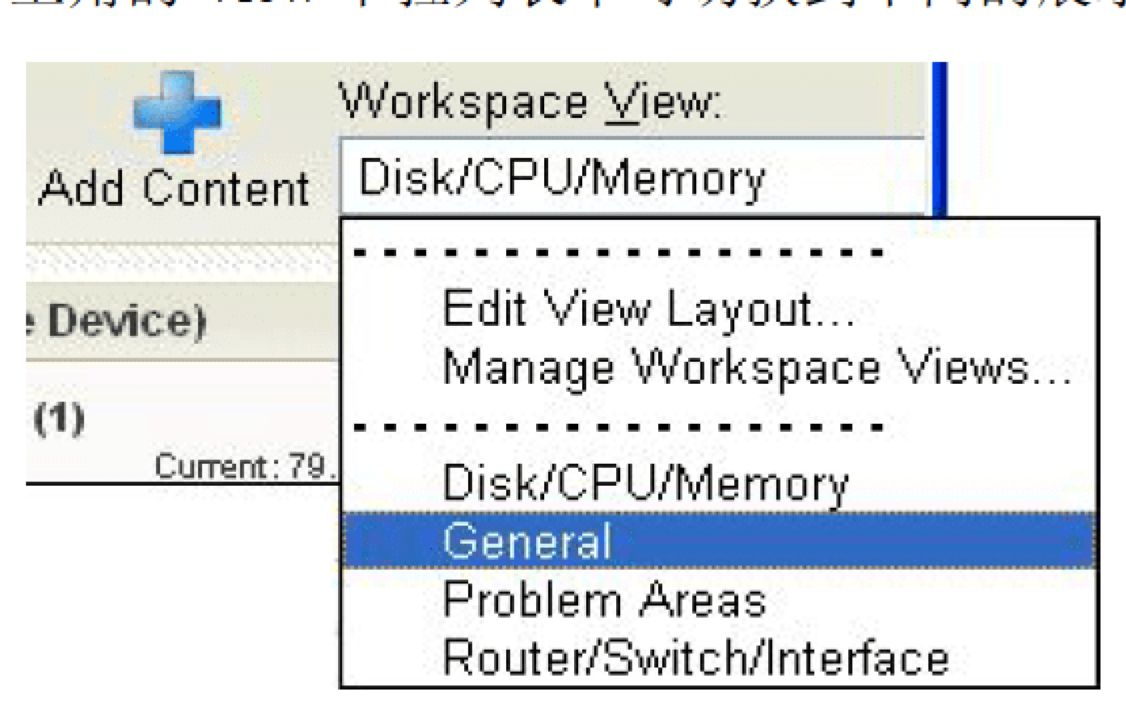


图 8-9　切换到不同的结构视图

以上 4 种样式中，只有 General 是包含综合信息的视图结构，另外 3 种均为展示单个设备信息界面。如果需要查看某个设备的 Disk/CPU/Memory，首先到 Device 设备页面中，选择需要查看的设备，双击该设备，即可进入到设备状态工作视图，然后在设图的 View 样式中选择 Disk/CPU/Memory 即可，如图 8-10 所示。如果未做设备选择，则直接进入该

视图样式，则将显示上次所选设备的信息。

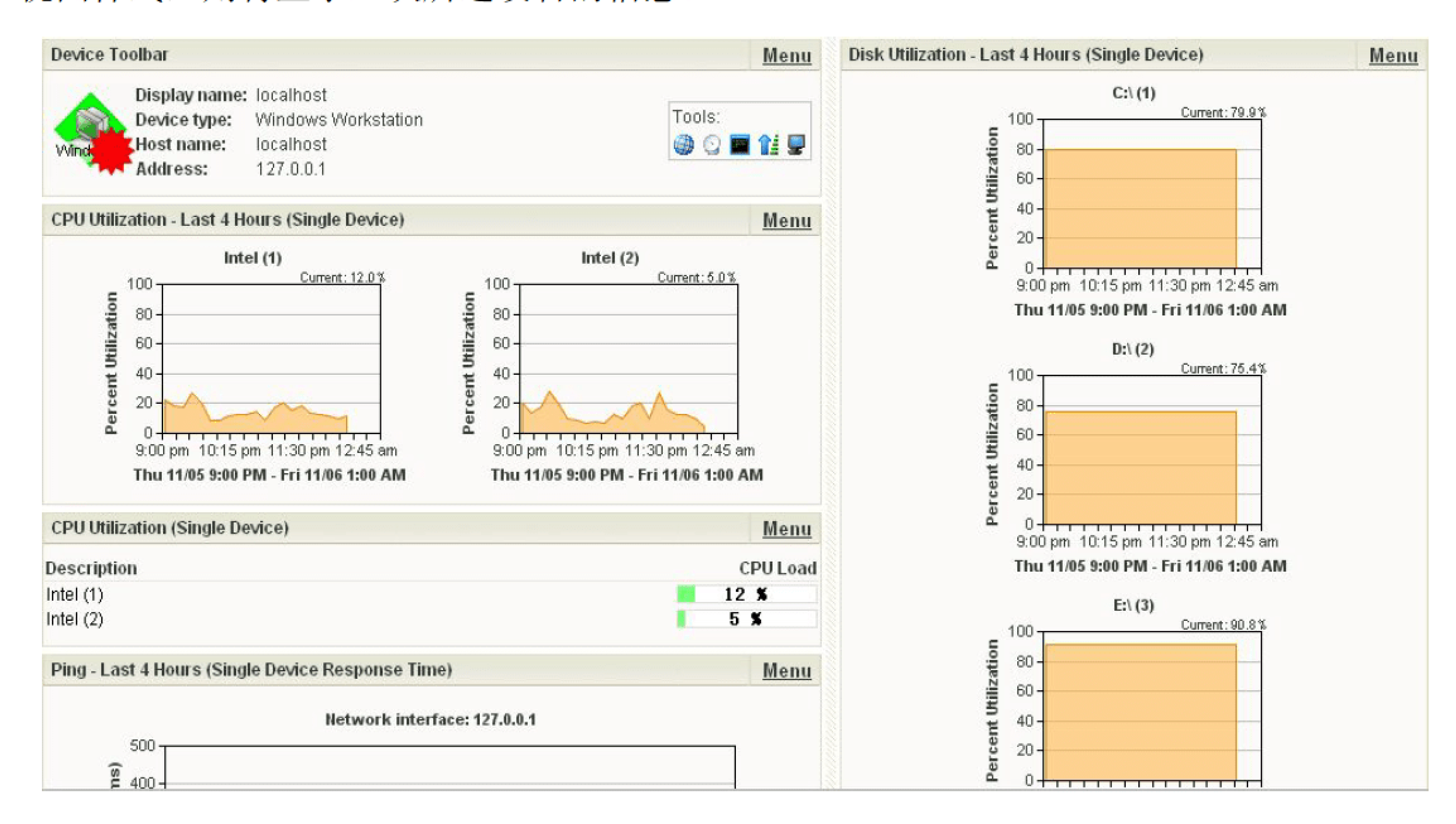


图 8-10　单一设备状态工作视图

设备状态视图便于了解单个设备的全面信息，例如，了解磁盘信息（如图 8-11 所示）、内存信息（如图 8-12 所示）、主动监测项目信息（如图 8-13 所示）等。

Disk Utilization (Single Device)　Menu

Description	Size Used	Total Size	Percent Used
C:\	11.79 GB	14.74 GB	79.9 %
D:\	18.56 GB	18.82 GB	98.6 %
E:\	17.79 GB	19.58 GB	90.9 %
F:\	25.07 GB	29.30 GB	85.6 %

图 8-11　某设备的磁盘信息

Memory Utilization (Single Device)　Menu

Description	Size Used	Total Size	Percent Used
Physical Memory	886.94 MB	2.47 GB	35 %
Virtual Memory	839.06 MB	6.32 GB	13 %

图 8-12　某设备的内存信息



Down Active Monitors (Single Device)　Menu

Monitor	State
Exchange Moniter	Down at least 20 min
FTP	Down at least 20 min
HTTP	Down at least 20 min

图 8-13　主动监测项目信息

8.1.4 Top 10 视图

Top 10 视图展示网络中按各种属性排名前 10 名的网络设备整体信息。Top 10 报表主要用于展现网络中异常状态的严重程度排名，它提供了如下 6 种数据排名信息。

- Interface utilization：接口占用率；
- Interface traffic：接口拥塞程度；
- Ping response time：Ping 操作响应时长；
- Disk utilization：磁盘占用率；
- CPU utilization：CPU 占用率；
- Memory utilization：CPU 占用率。

在 Home Workspace 界面中，点击 Favorite Reports 面板中的 Top 10 链接，即可打开设备按照各种硬件利用率排名，如图 8-14 所示。

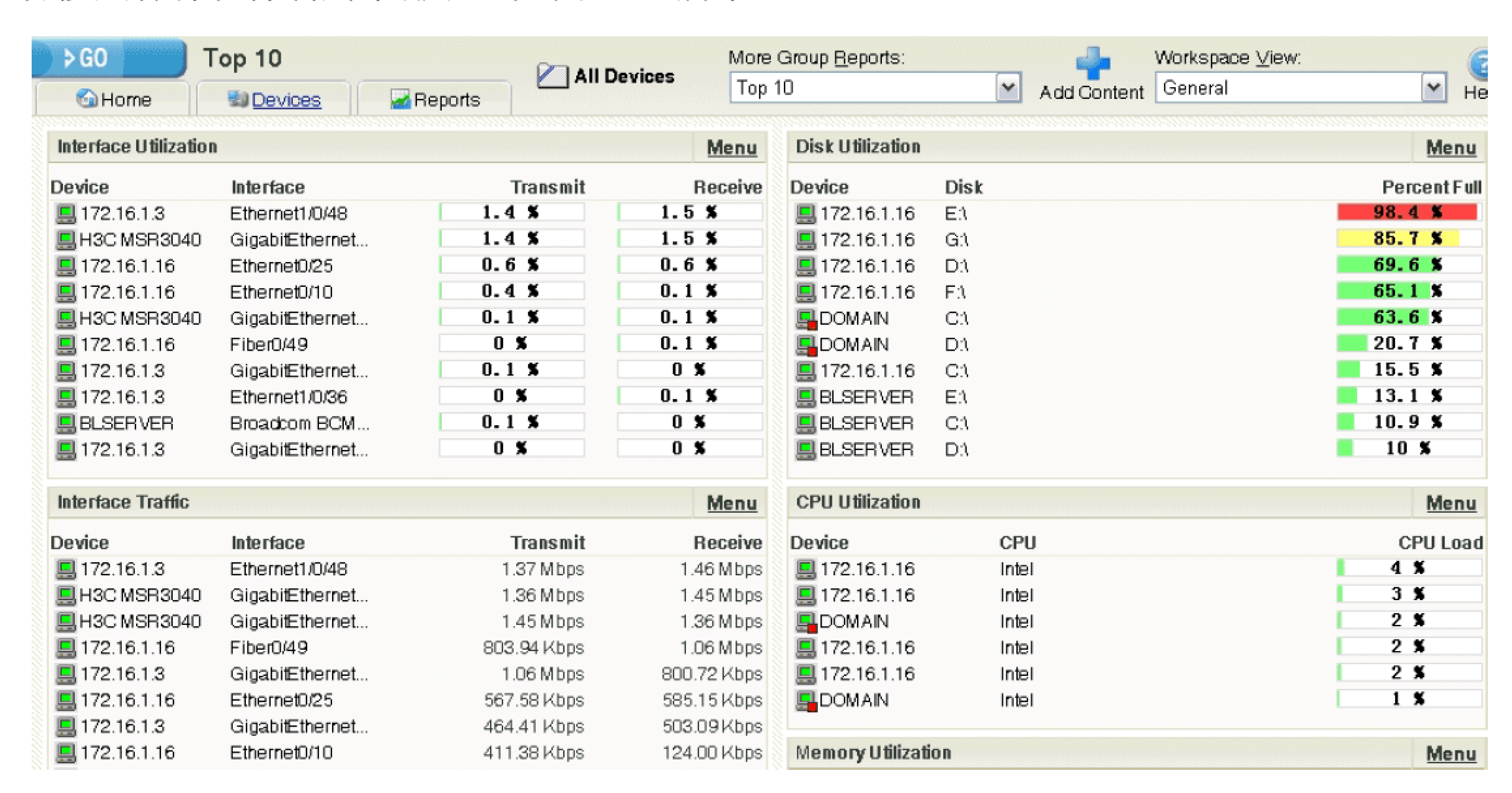


图 8-14 Top 10 报表信息

8.1.5 自定义新建视图

除了 Web 界面中自带的多种视图结构，还可以根据实际需要了解报表信息自定义视图。新建视图步骤如下：

（1）单击 Home 视图右上角的按钮打开 Workspace Views 下拉列表，选择 Manage Workspace Views（管理工作间视图）选项，打开视图管理界面，在该界面中，可编辑、删除现有视图，也可以通过复制实现视图的复制，如图 8-15 所示。

（2）单击 New 按钮，建立一个可配置的视图模式。在新建对话框中，输入新建视图的信息，包括视图名称、视图类型（Home、Device Status、Top 三种）类型选择及显示内容

分多少列（Column count）和宽度设置，如图 8-16 所示。

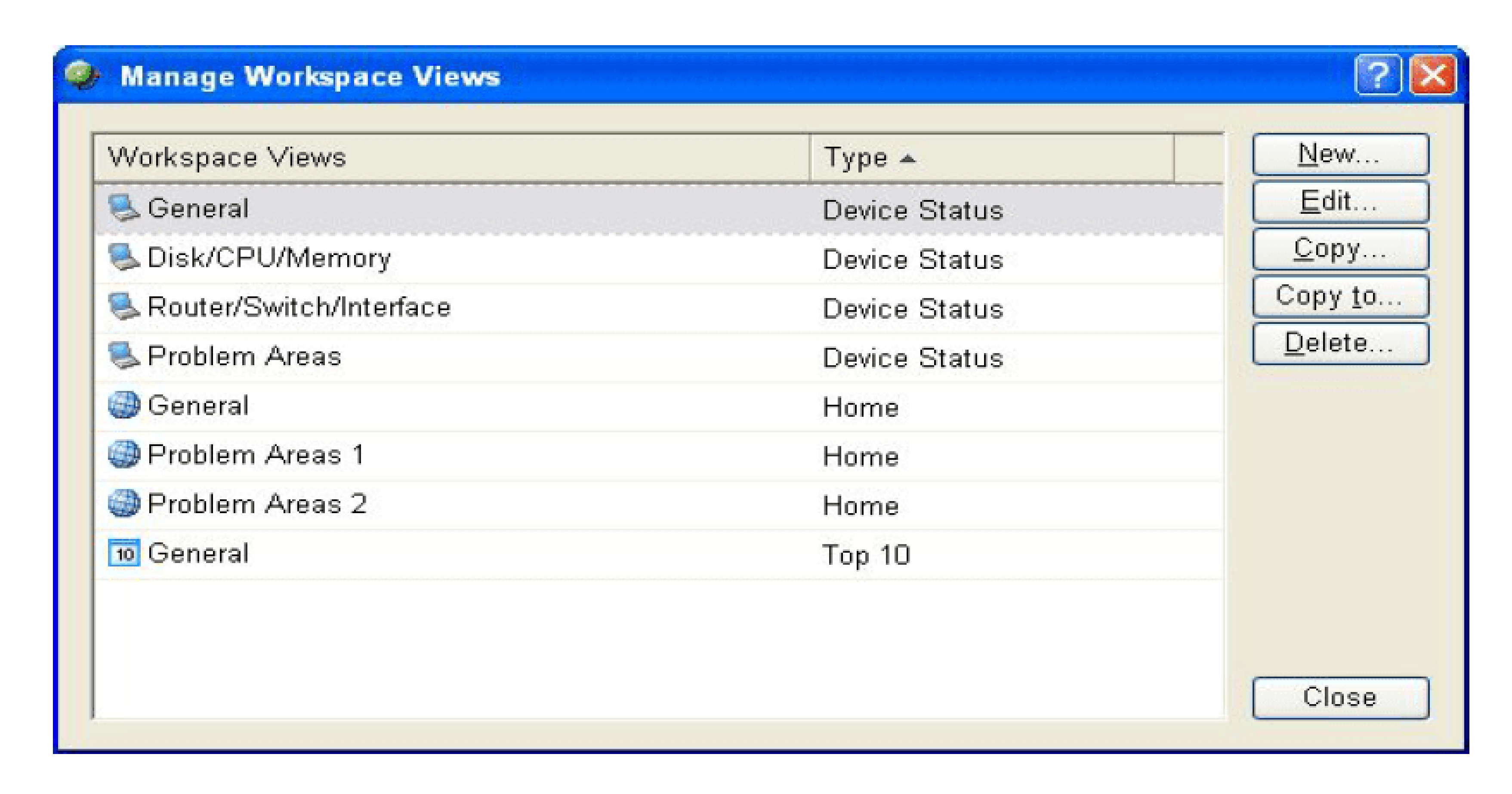


图 8-15　工作间视图的管理界面

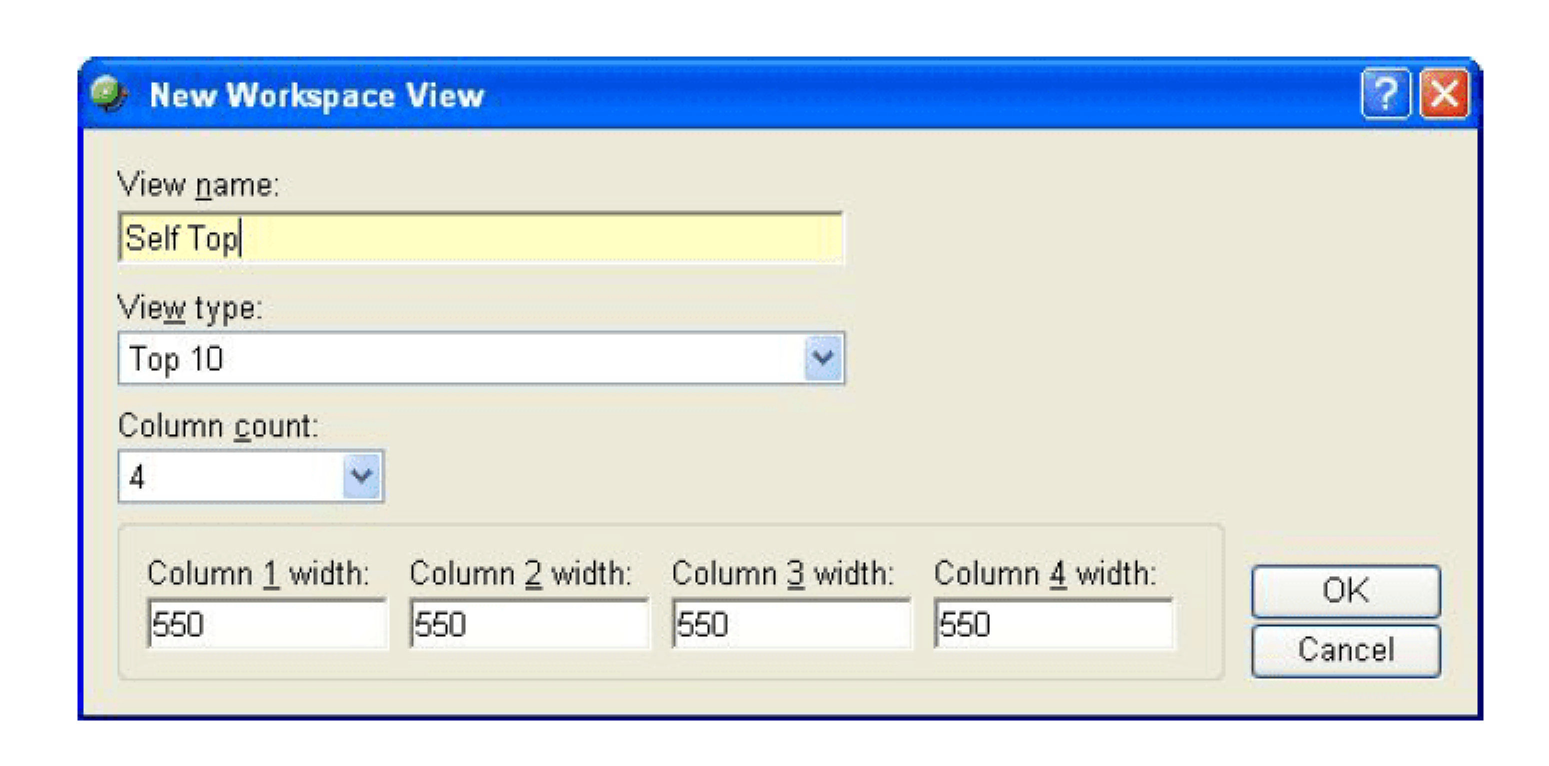


图 8-16　新建视图

（3）单击 OK 按钮确定后，将建立一个新的空白视图，然后为该视图添加显示内容。首先回到 Home 界面，在界面右上角选择 Workspace View 列表中刚创建的视图，并单击左侧的 Add Content 按钮，在打开的列表选项中添加需要展示的项目内容即可。

（4）如果需要对视图进行重新布局，则在 Home Workspace 界面中可对现有的各个显示区域重新排版布局，只需要选择某区域，然后拖放到新的显示区域即可，如图 8-17 所示。

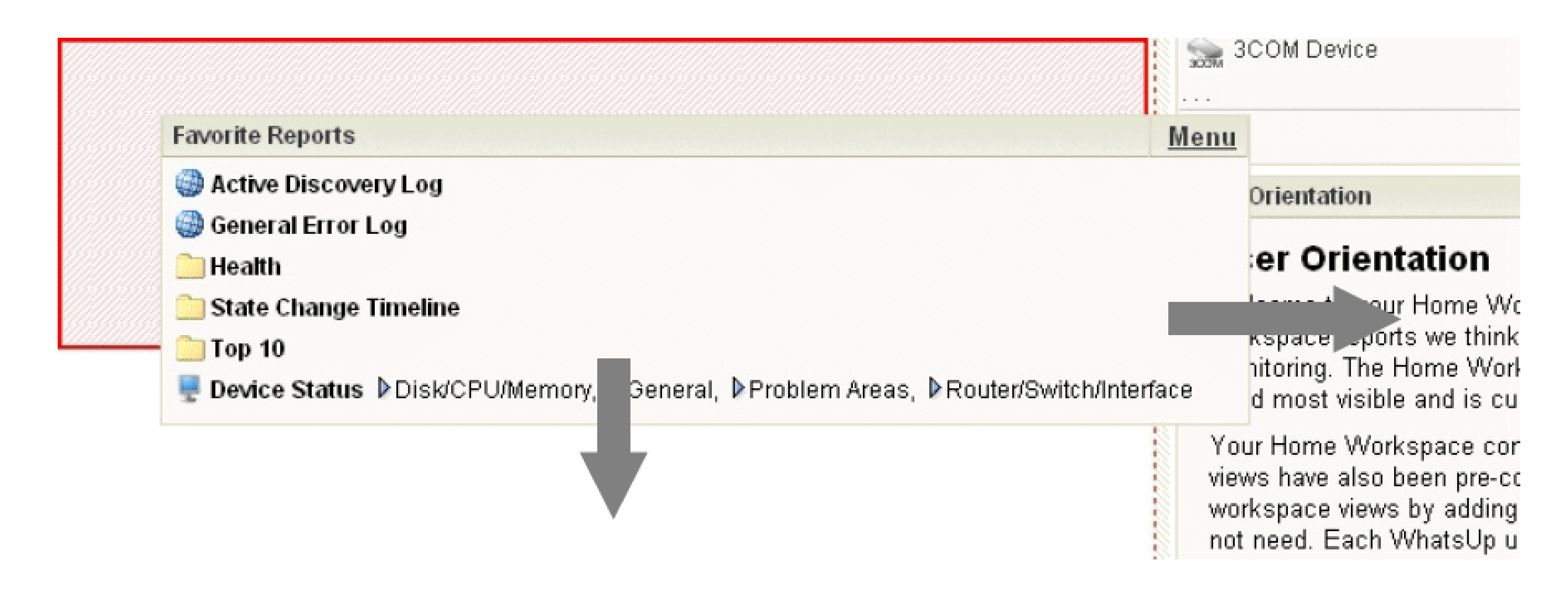


图 8-17　对显示区域重新布局

8.1.6 添加报表显示区域

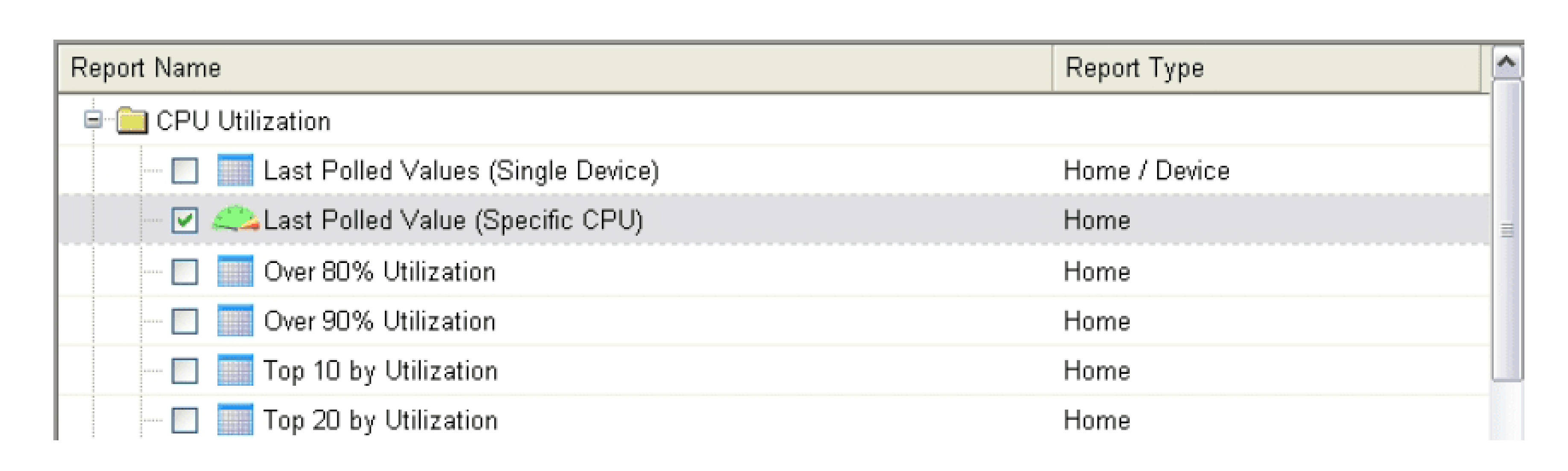
在 Home Workspace 页面，可根据用户关心的内容添加报表显示内容。此处举例添加某设备的 CPU 饼图和硬盘仪表盘图，通过图形直观地的了解该设备的资源占用率。首先添加 CPU 饼图，步骤如下：

（1）在视图右上角单击 Add Content 按钮（如图 8-18 所示），将弹出添加报表或图标的界面，可选择添加图表、数据表、曲线图等内容。



图 8-18 添加报表显示区域

（2）在弹出的界面中选择 CPU 利用率 CPU Utilization | Last Polled Value 选项，即查看上一次轮询设备获得的 CPU 利用率，如图 8-19 所示。



Report Name	Report Type
CPU Utilization	
Last Polled Values (Single Device)	Home / Device
Last Polled Value (Specific CPU)	Home
Over 80% Utilization	Home
Over 90% Utilization	Home
Top 10 by Utilization	Home
Top 20 by Utilization	Home

图 8-19 选择添加显示 CPU 利用率的报表区域

（3）确定选项后将在 Web 主界面中新增一块用于显示 CPU 属性的区域，如图 8-20 所示。

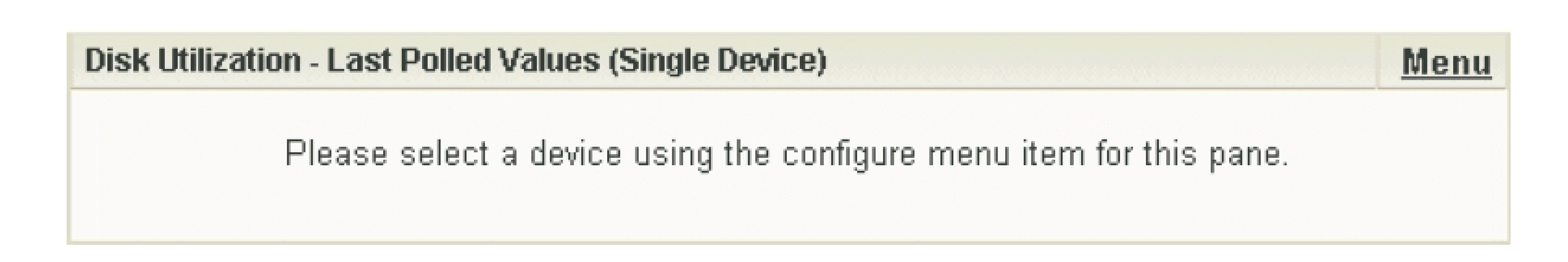


图 8-20 添加的新显示区域

8.1.7 配置显示内容

新添加的报表区域仅规定了显示内容，但并未为该区域指定具体的设备，所以此处还需要选择设备。操作步骤如下：

（1）选择该新增区域右上角的 Menu 菜单，打开菜单命令，选择 Configure 命令进行内容配置，如图 8-21 所示。

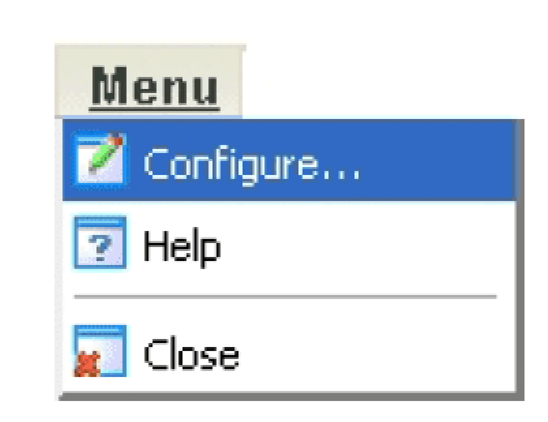


图 8-21 配置显示区域内容

（2）在 Configure 对话框中选择要显示 CPU 状态的对象主机，此处选择域服务器 Domain。在 Graph type 下拉列表中，有 Pie（饼图）、Gauge（仪表盘图）、Horizontal（水平标尺图）等种类供选择，此处选择 Gauge，展示 CPU 利用率情况，如图 8-22 所示。

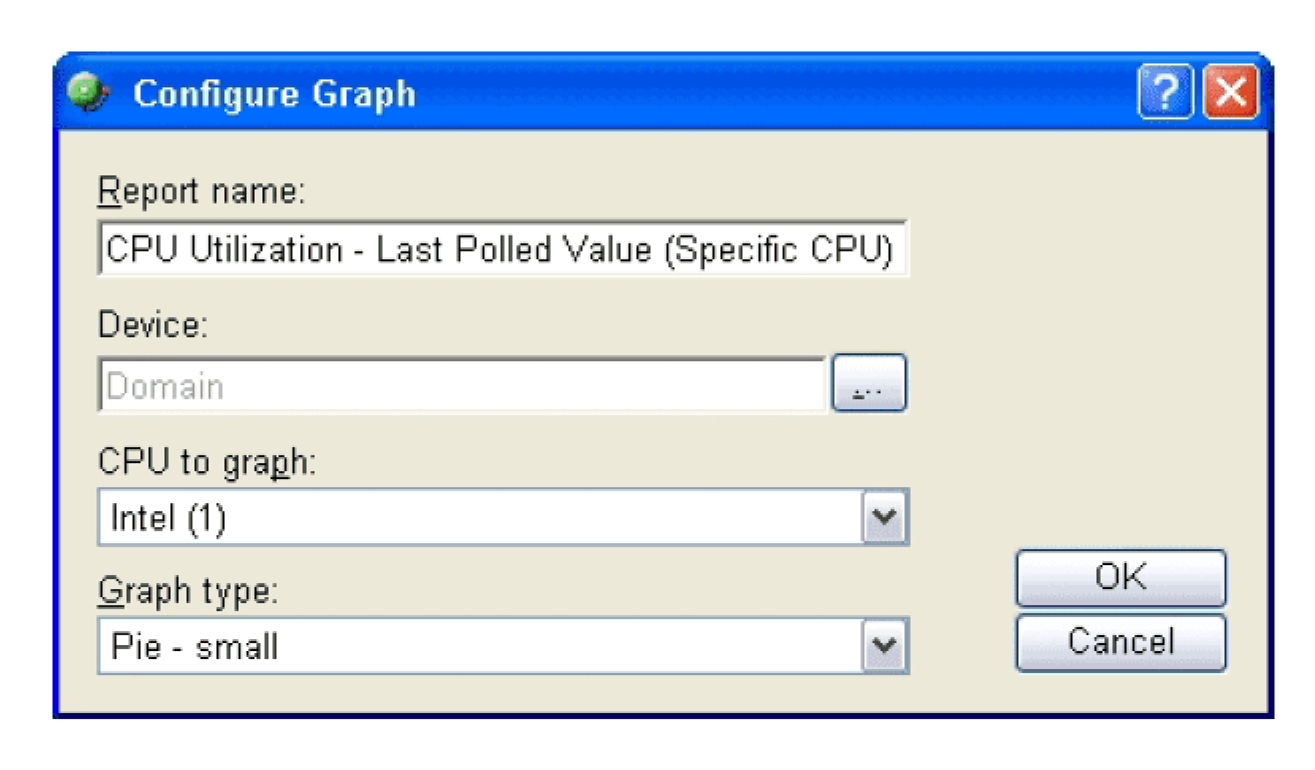


图 8-22　配置报表内容

（3）单击 OK 按钮确定后，即完成配置，在报表显示区域中将显示指定设备的 CPU 性能仪表盘，如图 8-23 所示。可看出该设备的 CPU 资源利用率较低，仅为 14%左右。

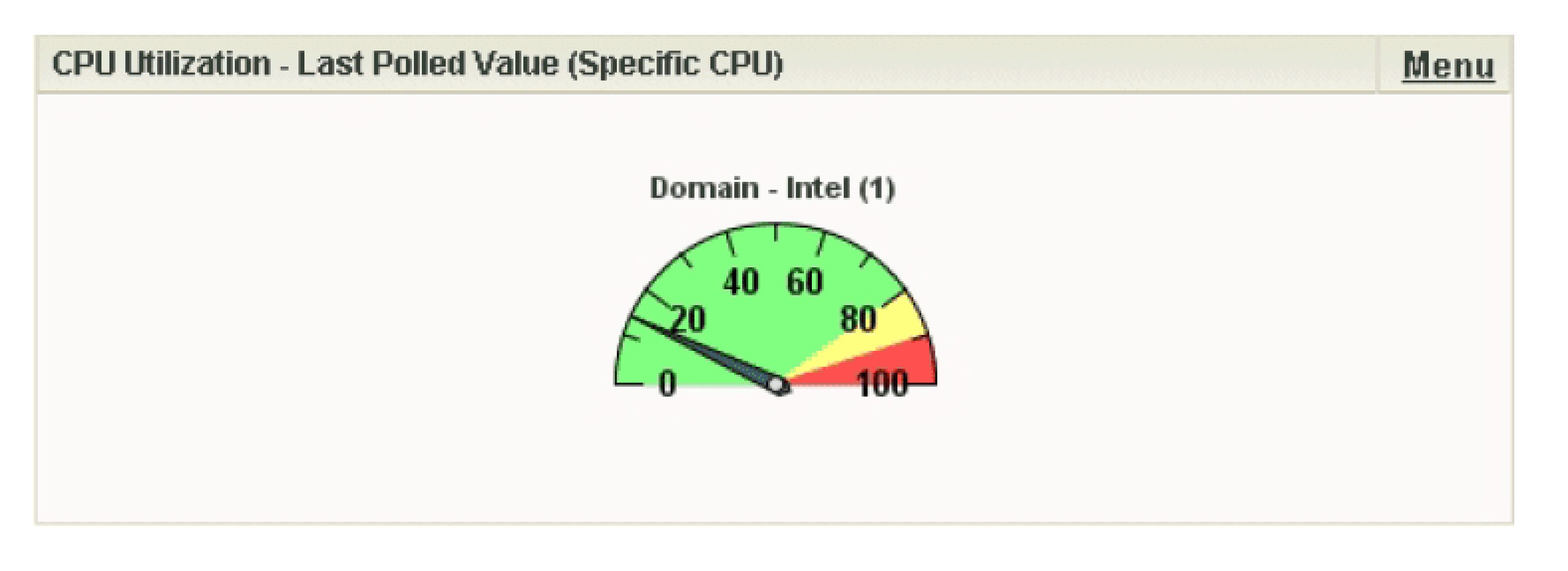


图 8-23　CPU 利用率图表

（4）用同样的方式，可添加磁盘容量的饼图。同样添加显示区域，再配置设备后，资源利用率图表展示如图 8-24 所示。可以看出，该设备磁盘中 C 盘的容量使用比例。

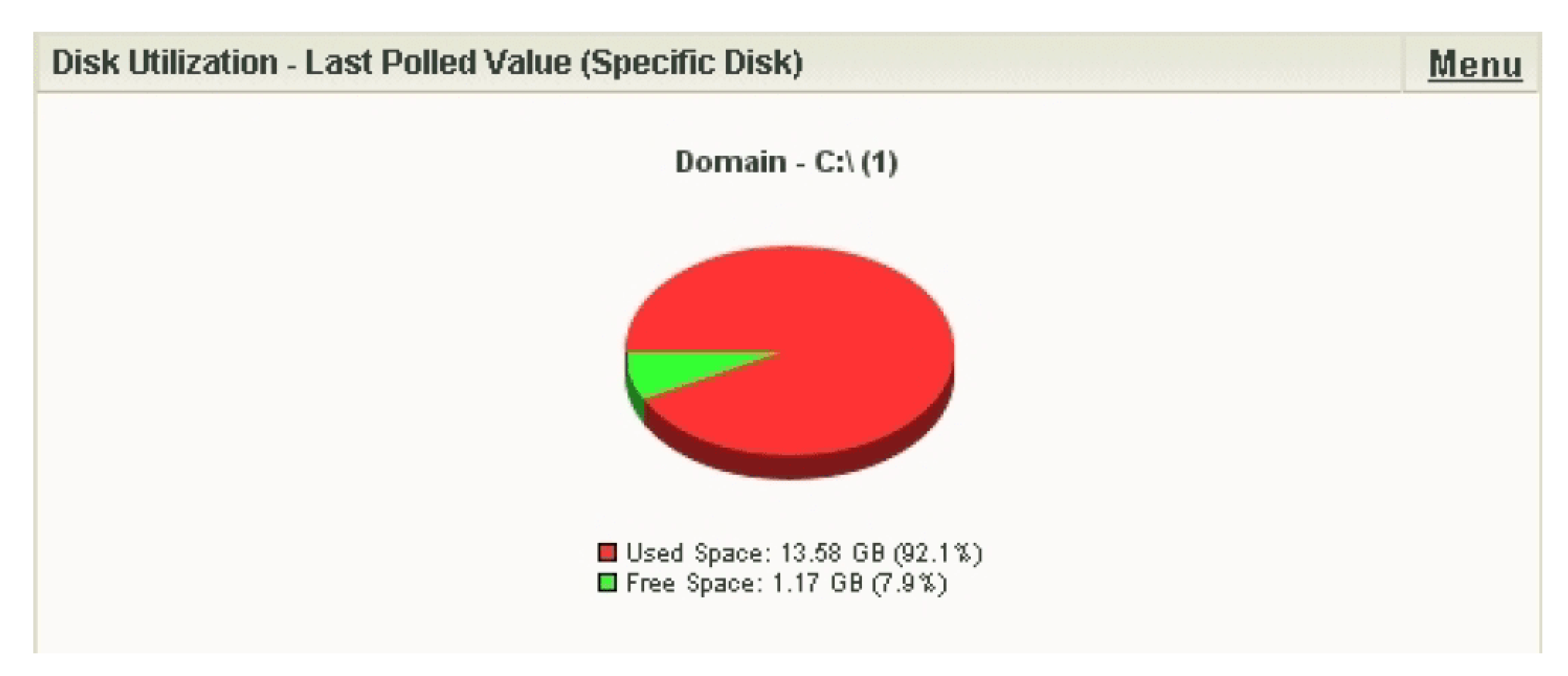


图 8-24　磁盘容量饼图

8.1.8 删除报表显示区域

如果需要删除某显示区域，则选择该区域右上角的 Menu 菜单并选择 Close 命令，即可在该视图中关闭所选区域，如图 8-25 所示。

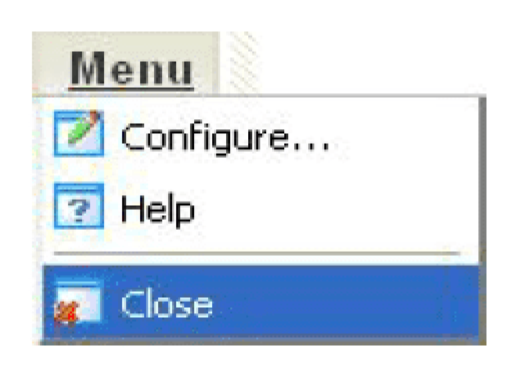


图 8-25 删除区域

8.2 Device 视图介绍

在 Web 主界面的 Device 选项页面中提供了和程序控制台管理界面一样的界面和功能。该界面就是控制台界面的克隆版本，同样列出了设备组及其包含的设备列表，如图 8-26 所示。

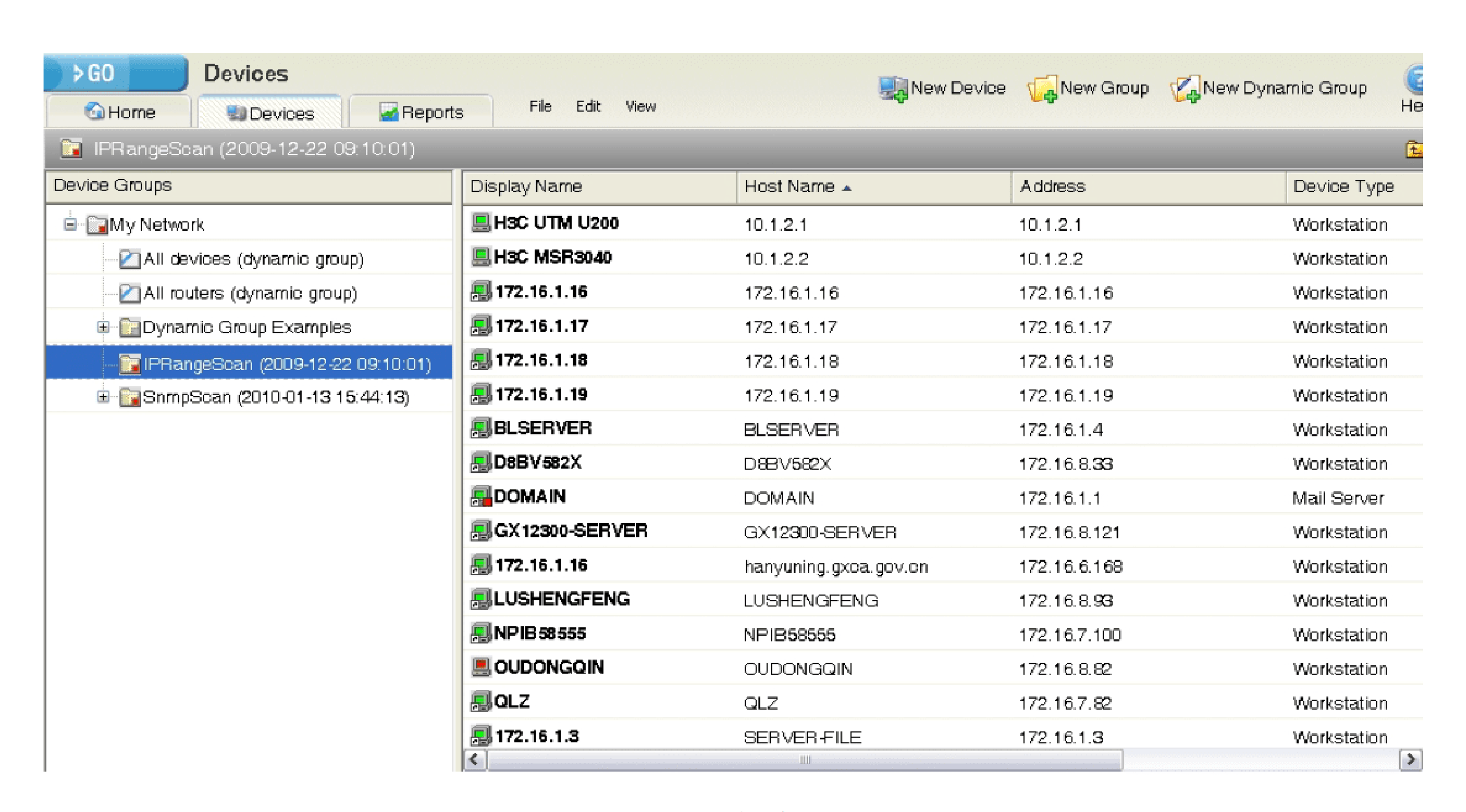


图 8-26 新建视图

同样，在某设备上右击，也能够打开其属性界面，可对其基本属性、监测内容等进行配置。配置信息将自动保存到数据库中。无论在控制台界面，还是 Web 界面，配置同样是同步生效的。Web 模式中设备属性界面如图 8-27 所示。

由于该界面与控制台界面功能完全相同，此处不再进行介绍。

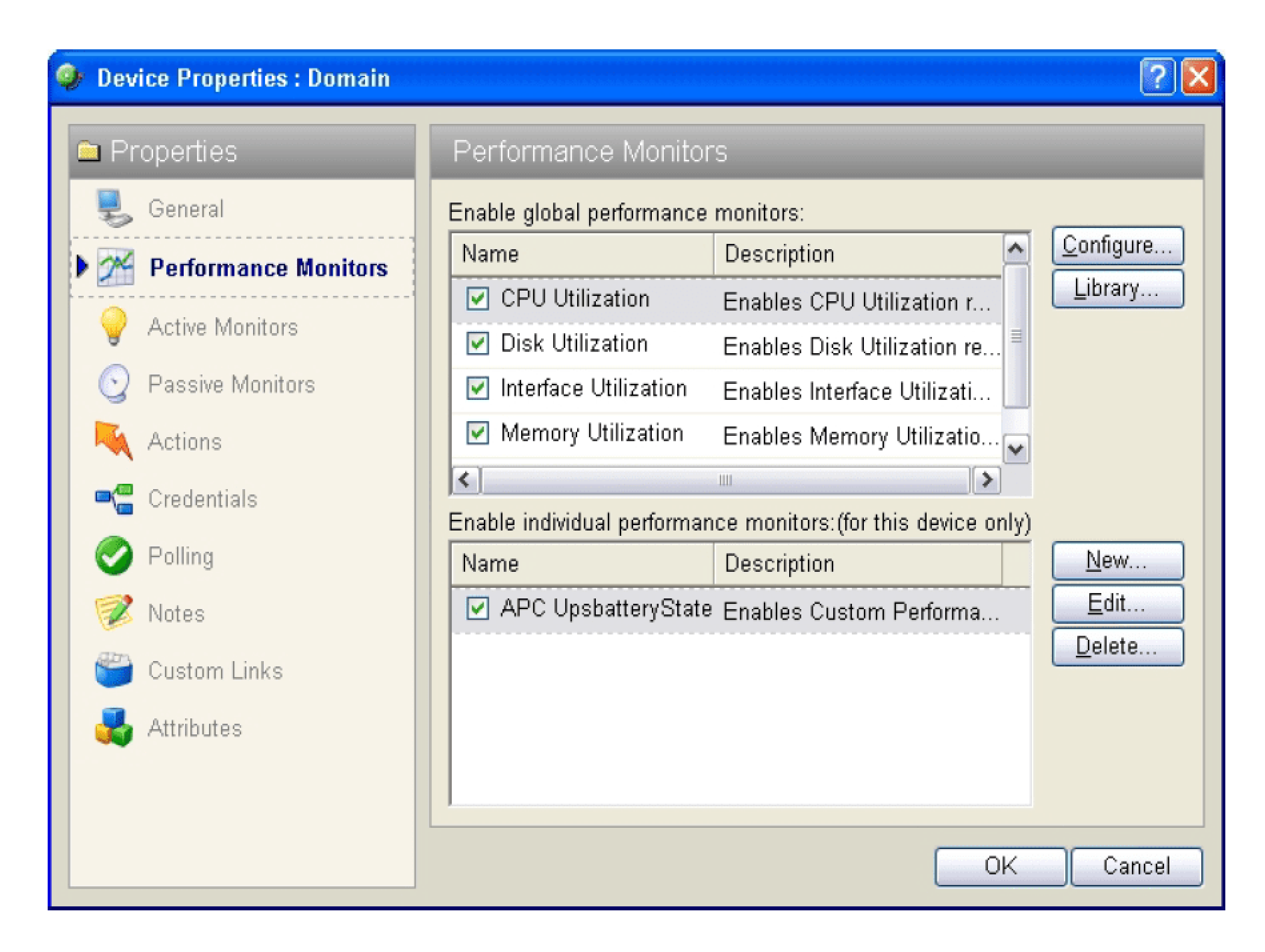


图 8-27 Web 界面配置设备属性

8.3 Report 视图介绍

8.3.1 Report 视图简介

报表用于展示在 WhatsUp Gold 运行过程中采集到的历史数据。这些报表能够帮助网管员了解网络长期运行状态，分析和优化网络结构。这些报表仅作为数据的展示，并不具备交互性，这些数据是无法被修改的。

在 Web 模式主界面中选择 Report 界面，可以看到 Web 模式提供了种类丰富的报表信息，如图 8-28 所示。

在 Report 界面中以图表方式列出了最常用的几种报表类型。

- The Active Discovery Log：主动发现设备日志，记录了主动发现任务的结果。
- The General Error Log：记录了常见的错误日志。
- Health：记录了某一组设备当前状态的“拍照”取值。
- The State Change Timeline：记录了某一组中所有设备状态变化情况的历史记录。
- The Top 10 Report：6 类常用参数值（例如磁盘利用率、CPU 利用率等）取值排名前 10 的信息报表。
- The Device Status Report：指定设备的各项信息明细报表。

网管员也可以根据自己的需要，补充或删除该列表中的报表类型。

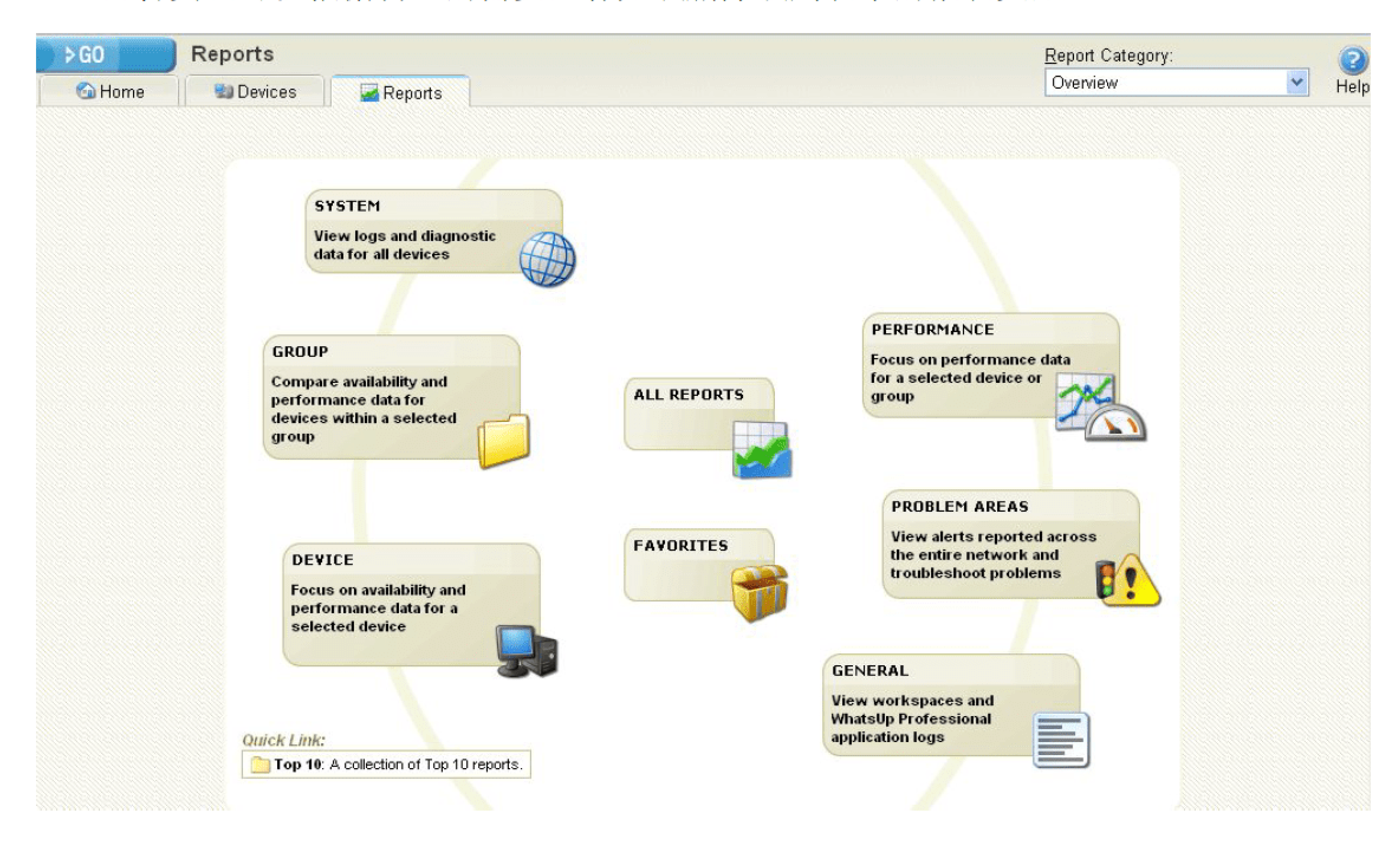


图 8-28　报表视图界面

8.3.2　报表类型和报表分类

在 Report 视图中选择右上角的 Report Category（报表分类）下拉列表，分类列出了报表不同类型，如图 8-29 所示。

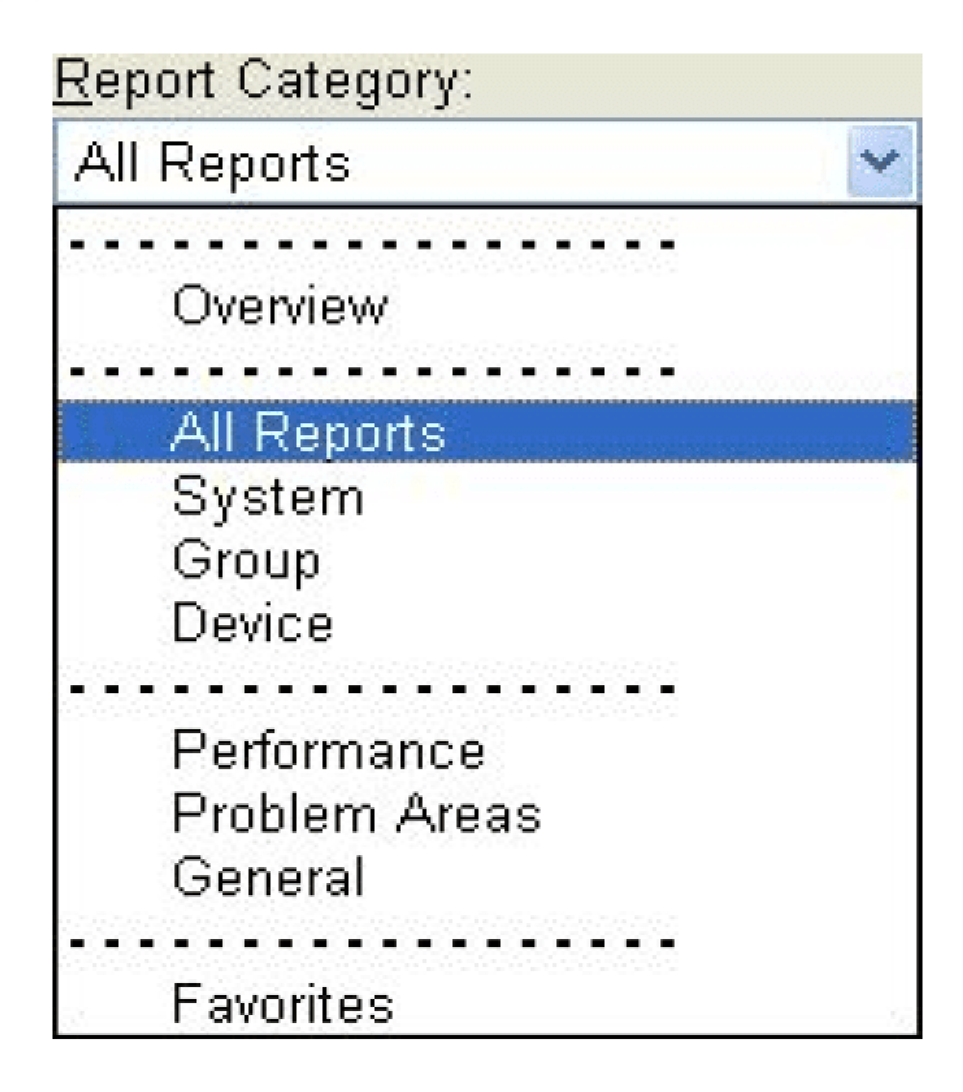


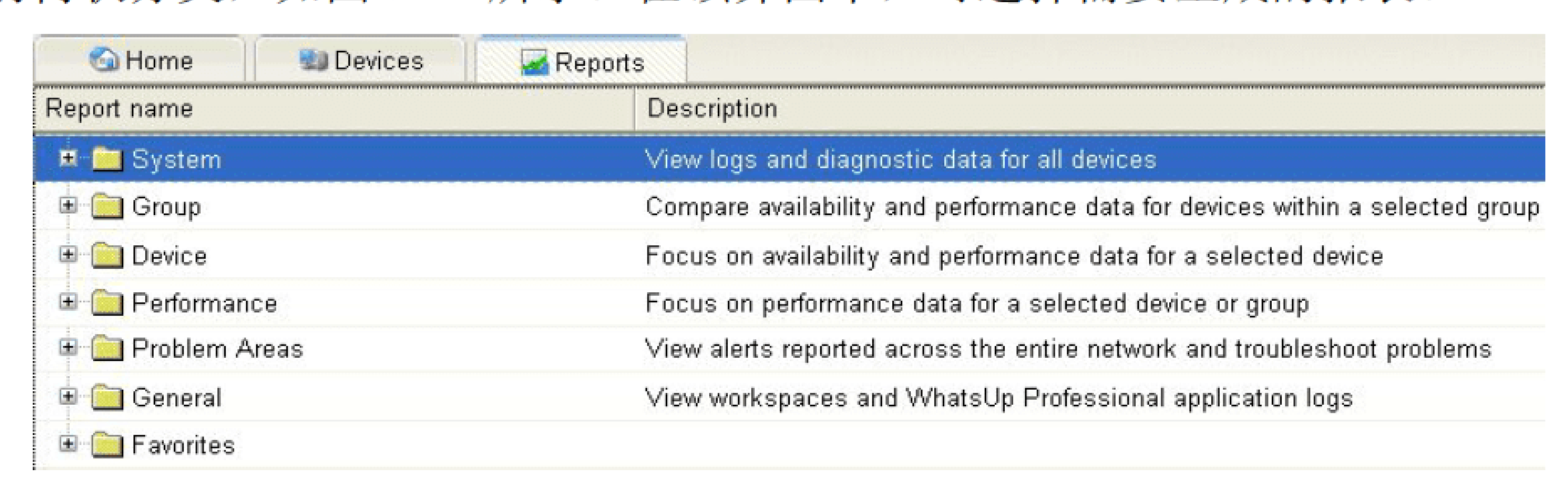
图 8-29　报表分类

在图 8-29 中，可以看到 WhatsUp Gold 提供的不同类型报表。

- System 报表：提供系统的完整信息。System 报表并不具体针对报表某一组设备或者某一单一设备。
- Group 报表：指定的设备组报表，例如设备组状态改变或针对该组设备的报警执行动作运用情况的报表。
- Device 报表：针对设备的信息报表，例如设备状态或设备性能监测结果。
- Performance（性能）报表：通过 WMI 和 SNMP 性能监视器获取信息的一类报表，其显示网络设备的 CPU、磁盘、接口和内存的利用率，以及 Ping 操作的反应时间和连通性。
- Problem Areas（故障区域）报表：故障定位报表，它通过分析各种日志记录报表审查网络故障。
- General 报表：显示应用程序设置和运行诊断，也包括设备属性和用户配置细节。

8.3.3 例图介绍常用报表

在 Report 视图中，选择 Report Category | All Report 选项，可看到 WhatsUp 提供的所有报表的树状分类，如图 8-30 所示。在该界面中，可选择需要生成的报表。

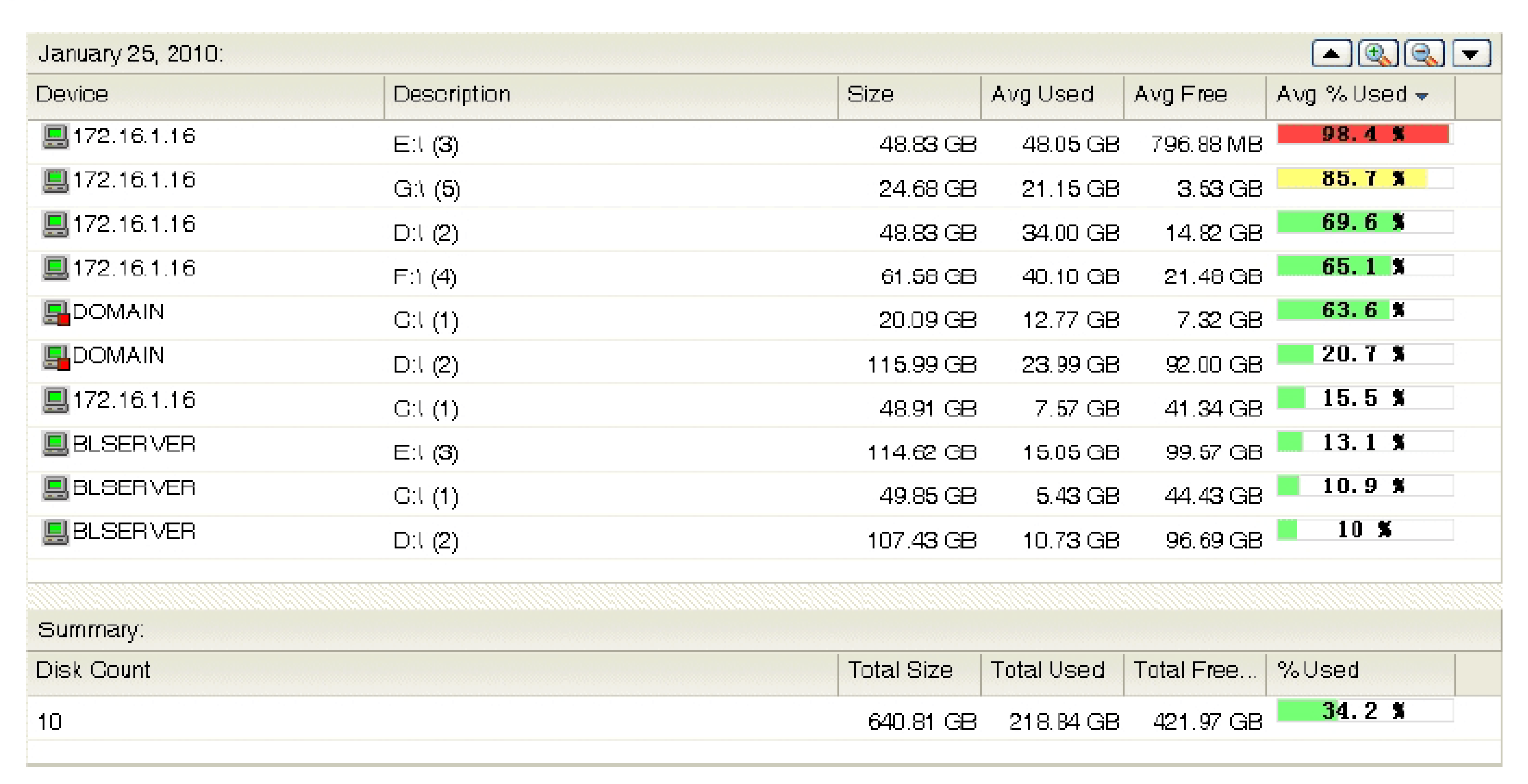


Home　Devices　Reports

Report name	Description
System	View logs and diagnostic data for all devices
Group	Compare availability and performance data for devices within a selected group
Device	Focus on availability and performance data for a selected device
Performance	Focus on performance data for a selected device or group
Problem Areas	View alerts reported across the entire network and troubleshoot problems
General	View workspaces and WhatsUp Professional application logs
Favorites	

图 8-30　查看所有的报表信息

在 Report 视图中，选择 Report Category | Group 选项，可查看设备组中的批量设备信息。在 Group 界面中选择查看磁盘信息，则列出了整组设备的磁盘利用率信息，便于实时了解设备的存储情况，如图 8-31 所示。



January 25, 2010:

Device	Description	Size	Avg Used	Avg Free	Avg % Used
172.16.1.16	E:\ (3)	48.83 GB	48.05 GB	796.88 MB	98.4 %
172.16.1.16	G:\ (5)	24.68 GB	21.15 GB	3.53 GB	85.7 %
172.16.1.16	D:\ (2)	48.83 GB	34.00 GB	14.82 GB	69.6 %
172.16.1.16	F:\ (4)	61.58 GB	40.10 GB	21.48 GB	65.1 %
DOMAIN	C:\ (1)	20.09 GB	12.77 GB	7.32 GB	63.6 %
DOMAIN	D:\ (2)	115.99 GB	23.99 GB	92.00 GB	20.7 %
172.16.1.16	C:\ (1)	48.91 GB	7.57 GB	41.34 GB	15.5 %
BLSERVER	E:\ (3)	114.62 GB	15.05 GB	99.57 GB	13.1 %
BLSERVER	C:\ (1)	49.85 GB	5.43 GB	44.43 GB	10.9 %
BLSERVER	D:\ (2)	107.43 GB	10.73 GB	96.69 GB	10 %

Summary:

Disk Count	Total Size	Total Used	Total Free...	% Used
10	640.81 GB	218.84 GB	421.97 GB	34.2 %

图 8-31　查看组设备的磁盘信息

例如，在 Group 界面，选择查看设备接口流量统计信息，如图 8-32 所示。

January 25, 2010:

Device	Description	Transmit %	Receive %	Avg Transmit	Avg Receive	Bytes Transm...	Bytes Received
172.16.1.3	Ethernet1/0/48 (4228002)	1.26 %	1.11 %	1.26 Mbps	1.11 Mbps	1.06 GB	959.29 MB
H3C MSR3040	GigabitEthernet0/1 (4)	1.25 %	1.12 %	1.25 Mbps	1.12 Mbps	1.05 GB	960.29 MB
H3C MSR3040	GigabitEthernet0/0 (3)	0.11 %	0.13 %	1.11 Mbps	1.25 Mbps	953.60 MB	1.05 GB
172.16.1.3	GigabitEthernet1/1/1 (4228041)	0.08 %	0.07 %	798.59 Kbps	715.96 Kbps	687.38 MB	616.25 MB
172.16.1.16	Fiber0/49 (6918)	0.07 %	0.08 %	716.11 Kbps	798.86 Kbps	616.31 MB	687.52 MB
172.16.1.16	Vlan-interface1 (7174)	N/A	N/A	716.11 Kbps	716.11 Kbps	616.31 MB	616.31 MB
172.16.1.16	Aux0/0 (390)	N/A	N/A	628.22 Kbps	628.22 Kbps	540.67 MB	540.67 MB
172.16.1.16	Ethernet0/25 (3590)	0.45 %	0.35 %	448.67 Kbps	354.15 Kbps	386.14 MB	304.79 MB
172.16.1.3	GigabitEthernet1/1/2 (4228049)	0.03 %	0.05 %	267.68 Kbps	482.85 Kbps	230.40 MB	415.60 MB
172.16.1.16	Ethernet0/10 (1670)	0.24 %	0.09 %	243.20 Kbps	91.87 Kbps	209.30 MB	79.07 MB
172.16.1.3	GigabitEthernet1/1/3 (4228057)	0.01 %	0 %	118.35 Kbps	17.26 Kbps	101.87 MB	14.86 MB
BLSERVER	Broadcom BCM5708C NetXtreme I...	0.07 %	0.01 %	69.10 Kbps	10.36 Kbps	59.48 MB	8.92 MB
172.16.1.16	Ethernet0/34 (4742)	0.06 %	0.01 %	59.98 Kbps	11.87 Kbps	51.62 MB	10.22 MB
DOMAIN	Broadcom BCM5708C NetXtreme I...	0.05 %	0.02 %	50.60 Kbps	22.79 Kbps	43.57 MB	19.62 MB

图 8-32　查看组设备的磁盘信息

在 Device 页面中，查看单个设备的信息报表。例如，选择路由器 H3C MSR3040，打开报表显示界面。首先在上方选择 Interface Utilization，然后选择路由器接口及时间范围，单击 Go 按钮，将显示指定接口的流量信息，如图 8-33 所示。

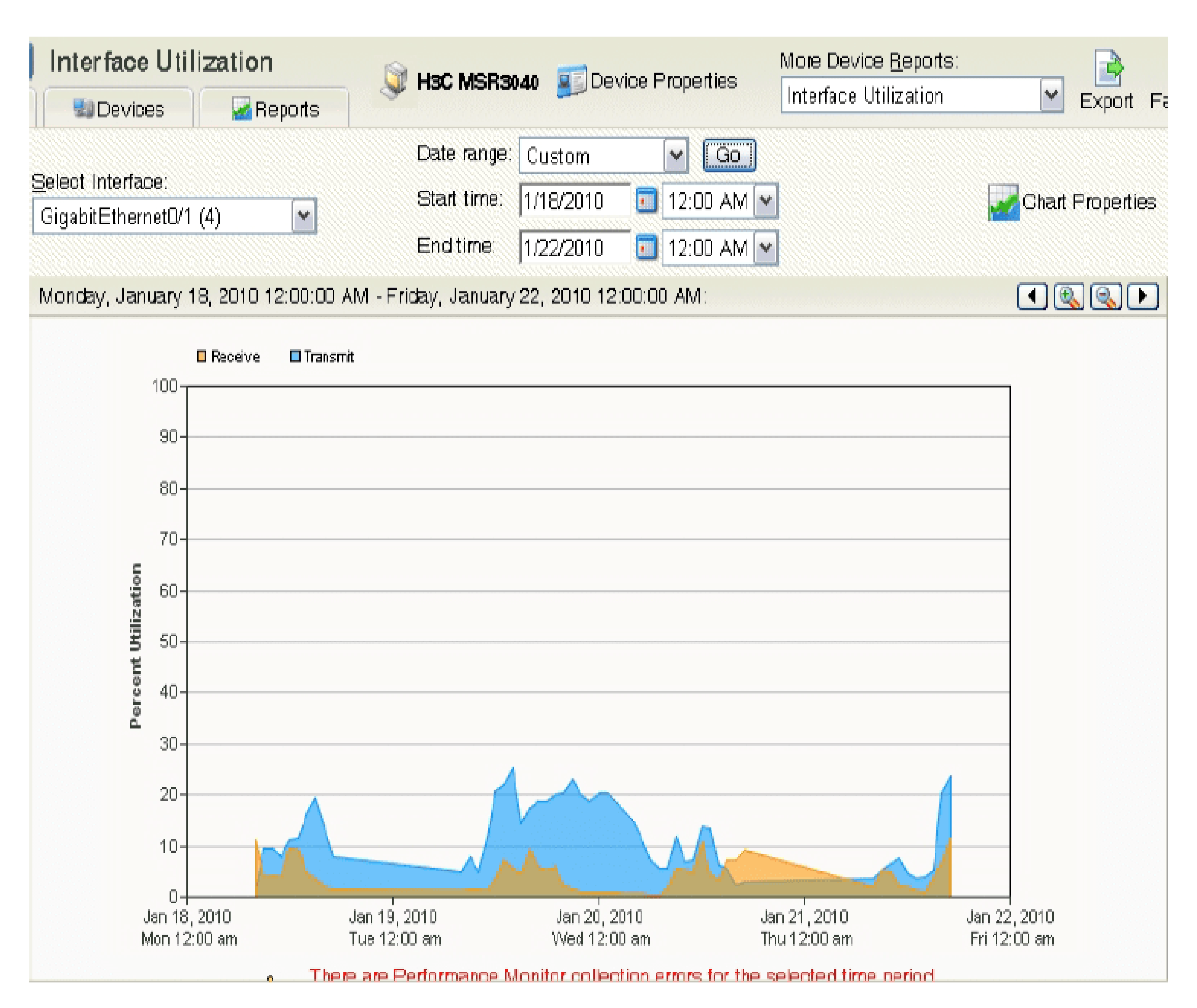


图 8-33　查看组设备的磁盘信息

以上报表均可导出至 Excel 中。单击报表界面右上方的 Export 按钮（如图 8-34 所示），即弹出导出窗口（如图 8-35 所示），可选择导出文件为 Text 文本或 Excel 文本。



图 8-34　选择导出报表

Export Report

Export to Text　Export to Excel

Include report title

Include column names

Text options:

Column delimeter: Comma

Text qualifier: Double Quote

OK

Cancel

图 8-35　选择导出报表类型

8.4 本章小结

通过本章的学习，读者可以掌握 WhatsUp Gold 的 Web 模式报表及应用。要熟练应用好网管程序管理网络，就需要深入了解主机对象、主机中运行的服务进程、监测机制的原理、获取数据的意义等，这样才能使用网管程序获得真正需要的、有用的监测信息。而且要能够根据需要生成期望的报表信息。

第 9 章　PRTG 安装及配置流量监测

本章首先对网络流量监测工具 PRTG（Paessler Router Traffic Grapher）的功能、特点和安装做简单介绍，使网管员对该工具的功能、安装步骤和应用环境有初步的了解。然后介绍使用 PRTG 查找和添加监测节点的操作过程，并对各种监测方式和相关难点做详细介绍。通过本章内容，网络管理员可将 PRTG 程序快速地应用在网络环境中。

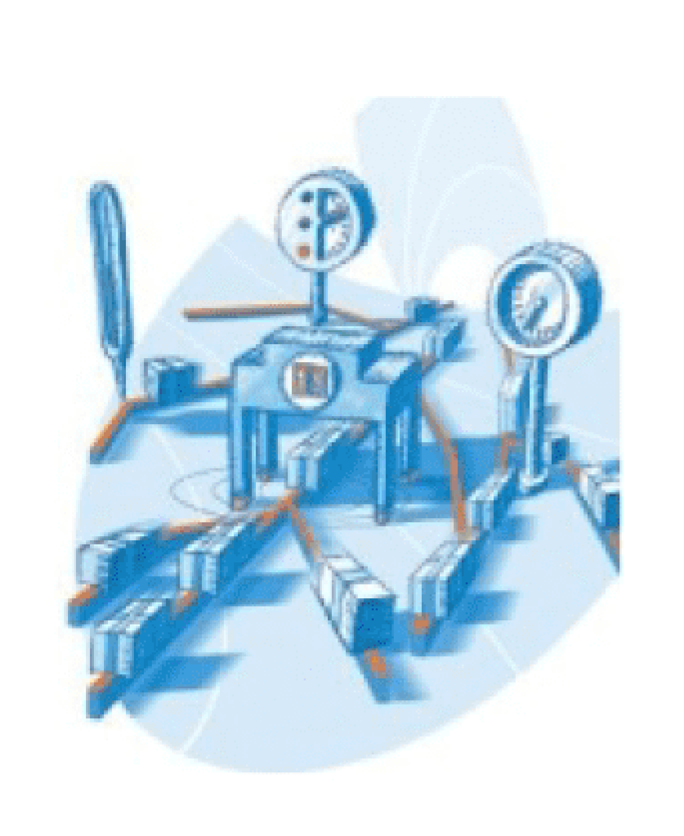
本章内容如下：

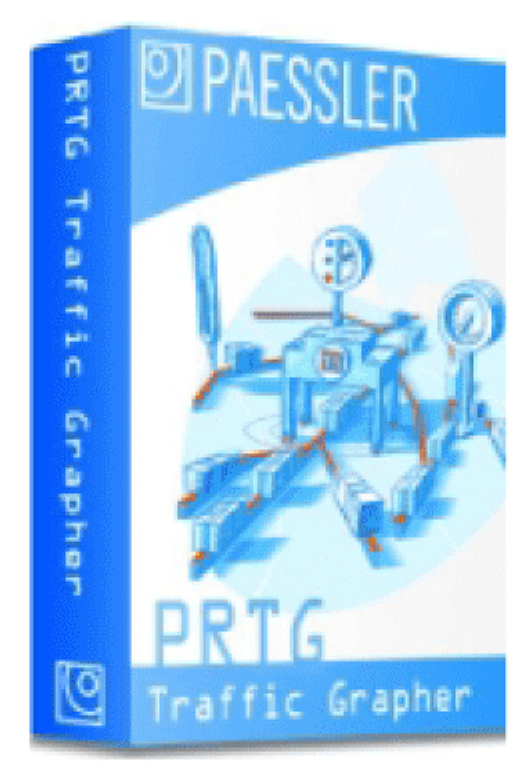
- ❑ PRTG 功能简介及安装指南；
- ❑ PRTG SNMP Helper 简介及安装指南；
- ❑ PRTG 涉及的技术概念；
- ❑ PRTG 查找和添加网络监测节点。

9.1　PRTG 简介及安装

目前，各行各业都或多或少地依赖于计算机和网络基础设施办公，保证网络和计算机的可靠性和高效性就变得至关重要。对于网络管理员，意味着必须保证网络的正常、稳定和高效运行，那么监测网络整体流量状态的手段不可或缺。

PRTG 程序用来监测网络和带宽使用状况及各种网络设备性能参数，如内存、CPU 使用率等情况。网管员可通过该程序了解网络实时数据交互状况，分析网络运行趋势，重新调整和配置路由器、防火墙、服务器和其他网络组件的使用，实现网络的优化，保障网络健康运行。该程序的图标如图 9-1 所示。





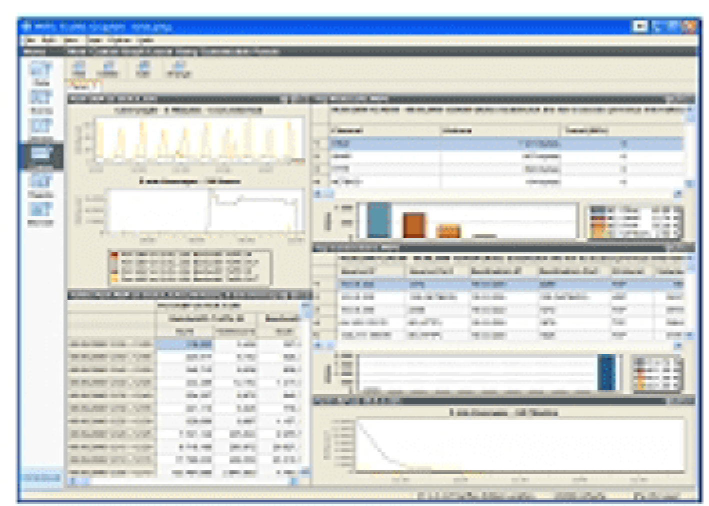


图 9-1　PRTG 程序图标

9.1.1 功能概述

PRTG 监测、记录和分析网络的流量数据，提供关于网络流量状态和使用趋势的精确数据，并通过各种直观易读的曲线图和表格显示结果，同时能够根据用户的需要自定义报表。

RPTG 通过 SNMP、数据包探测或 Cisco NetFlow 方式监测网络带宽使用及其他网络参数。通过简单的配置，能够监测流经路由器、网络专线的流量数据统计。同时，也能够监测其他支持 SNMP 协议的网络设备（如服务器、交换机、打印机等）的性能参数（如 CPU 利用率、磁盘利用率等）。

PRTG 主界面中可显示同一节点不同时段流量，也可同时显示多个节点的流量监测。节点的流量数据或性能参数可通过曲线图表进行展示，如图 9-2 所示。

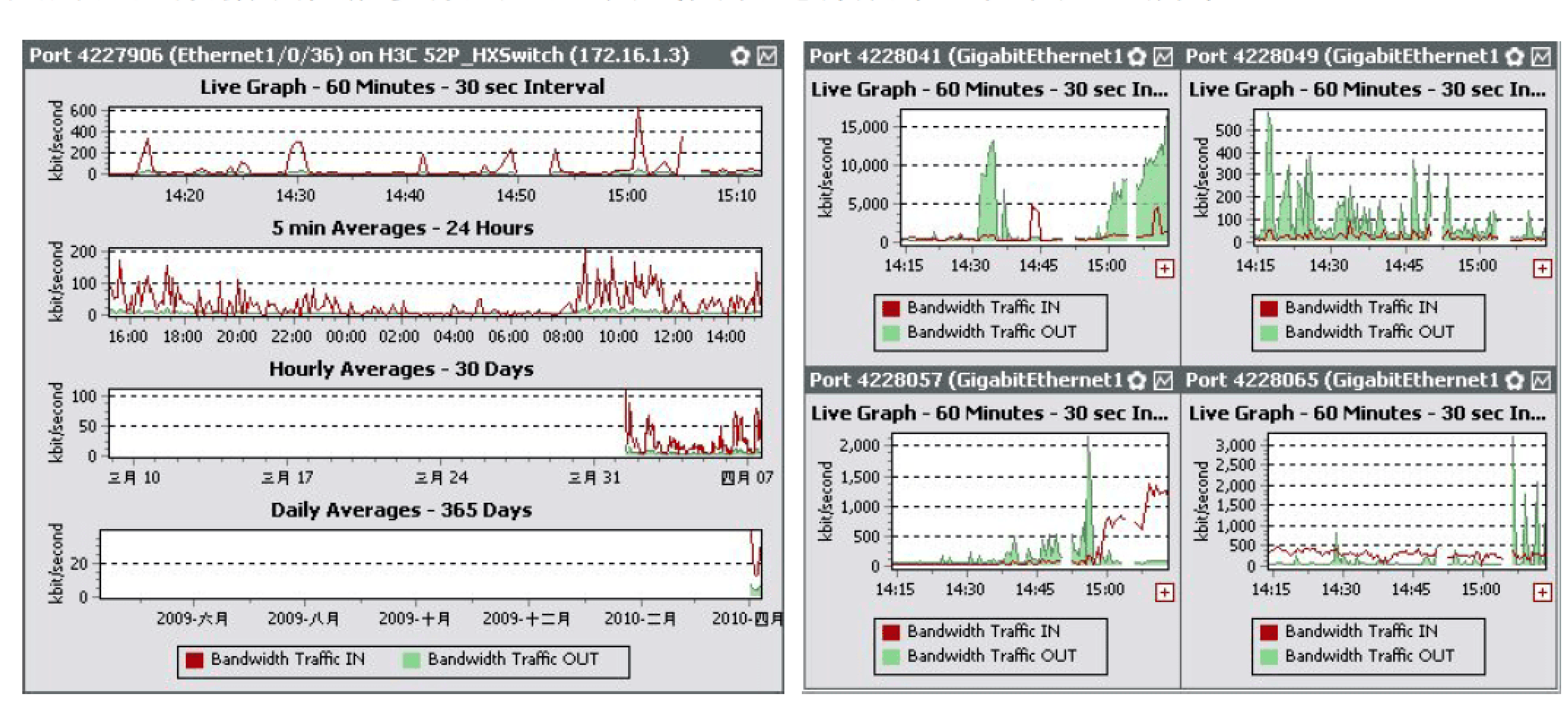


图 9-2　PRTG 流量监测生成的曲线图表

PRTG 数据采集通常使用 3 种常用的方式。

- SNMP：是 PRTG 采集数据和带宽信息的基础方法，它使用 SNMP 访问和监测路由器与交换机的每一个端口以获取流量信息。该模式需要被监测设备包含 SNMP v1、v2 或 v3 版本协议，并要求开启 SNMP 协议，以及允许安装 PRTG 的服务器访问被监测设备的接口。
- Packet Sniffing：数据包探测方式，它监测和检查流经（进入和流出）本地计算机网卡的数据包，并通过 IP、协议类型或其他参数对数据包进行分类统计。同时，该模式可监测网络核心交换设备的各个端口流量。
- NetFlow：大部分 Cisco 路由器支持 NetFlow 协议，PRTG 分析思科网络设备发出的 NetFlow 数据流，同样能对数据进行分类。该模式下的被监测设备必须配置为向 PRTG 主机发送 NetFlow 数据包（NetFlow5 版本），同时要求运行 PRTG 的主机安装 NetFlow 采集程序。

9.1.2 PRTG 特点

- 能够按照 IP 地址、协议或者其他参数对网络流量分类统计；
- 能够监测大多数的交换机、路由器、防火墙和其他网络设备；
- 安装于 Windows 2000/XP/2003 操作系统并易于使用；
- 监测引擎有能力监测超过数千个节点；
- 为监测数据提供各类报表；
- 节点的故障或超负荷时，发出报警信息；
- PRTG 可使用 Windows 图形界面程序和 Web 页面视图两种。

9.1.3 版本信息

提供免费版本（Freeware Edition）和商业版本（Commercial Editions）。免费版本可供个人用户和商业使用，但该试用版仅提供监测 3 个节点的功能（监测 3 个设备或 1 个设备的 3 个接口）。商业版本需要购买使用许可，可通过访问 PRTG 的官方网站 Http://www.paessler.com/，通过在线支付的方式购买许可注册码，或通过授权代理商处购买正版程序。

9.1.4 系统要求

本书中以 PRTG 6.0.6.675 版本做介绍。该版本可安装在 32 位和 64 位的 Windows 操作系统上，包括 Windows 2000/XP/2003 上。PRTG 运行需占用内存约 64MB，安装程序占用约 20MB 磁盘空间。但随着监测节点的增加和数据的增加，每个节点每日需要占用 300KB 的数据库容量，PRTG 将不断占用更大的磁盘空间。

9.1.5 安装指南

通过网络下载 PRTG 6.0.6.675 试用版或者通过软件提供商购买正版 PRTG，在安装程序之后需要输入注册码进行注册。PRTG 安装简单，以下为程序安装步骤。

（1）选择 PRTG 安装包，进入安装界面，如图 9-3 所示。

（2）单击 Next 按钮进入安装路径选择界面，如图 9-4 所示。

（3）单击 Next 按钮，进入 Windows 防火墙和 PRTG 检测插件选择界面。在 Windows Firewall Setup 中选择默认的 Enable network access to PRTG’s webserver 选项，即允许通过网络远程访问 PRTG 的 Web 管理界面。在 PRTG Watchdog Installation 中选择默认的 Install the PRTG Watchdog Service 选项，将安装 PRTG 自带的监测插件，能够获取网络更多信息，如图 9-5 所示。

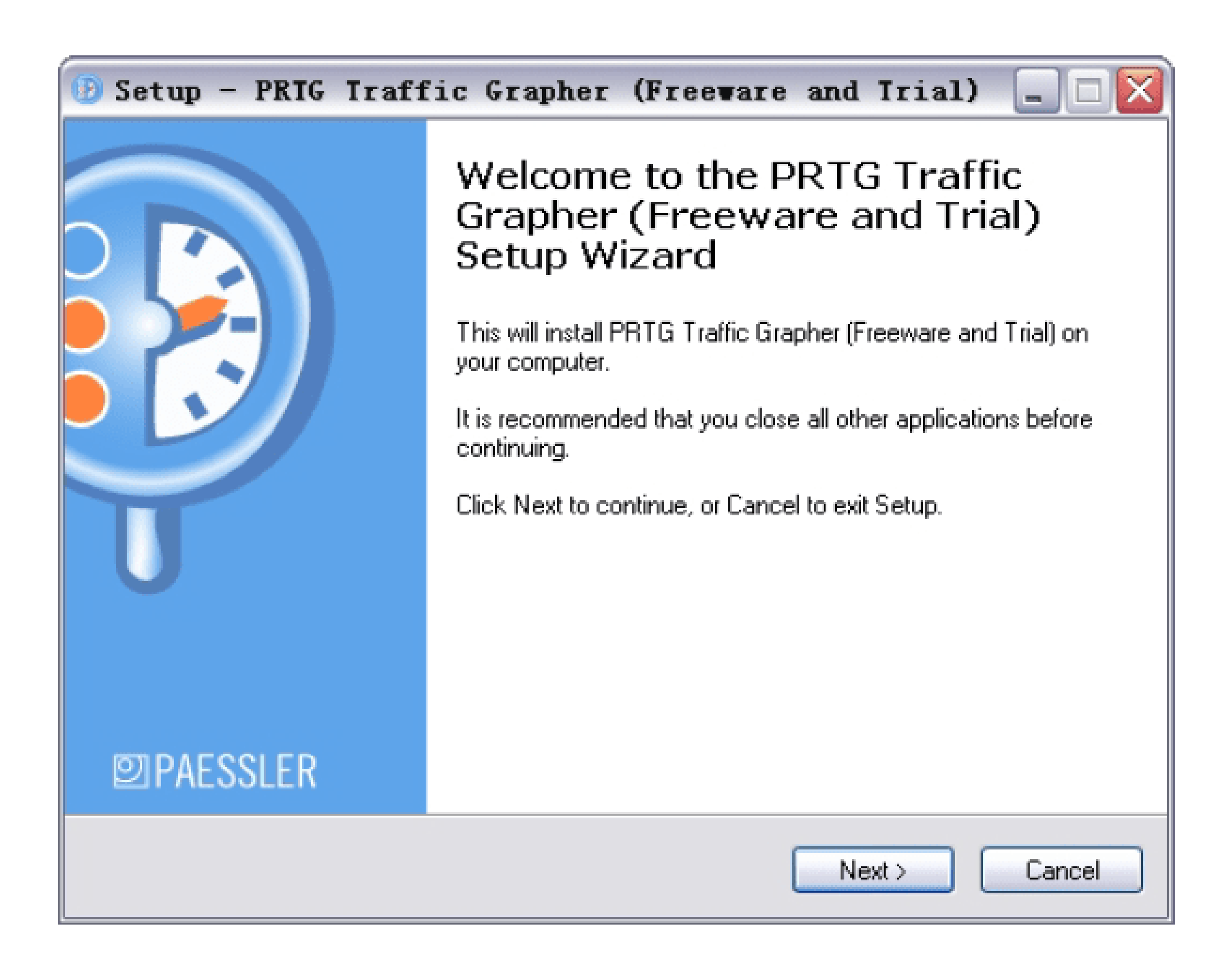


图 9-3　PRTG 安装界面

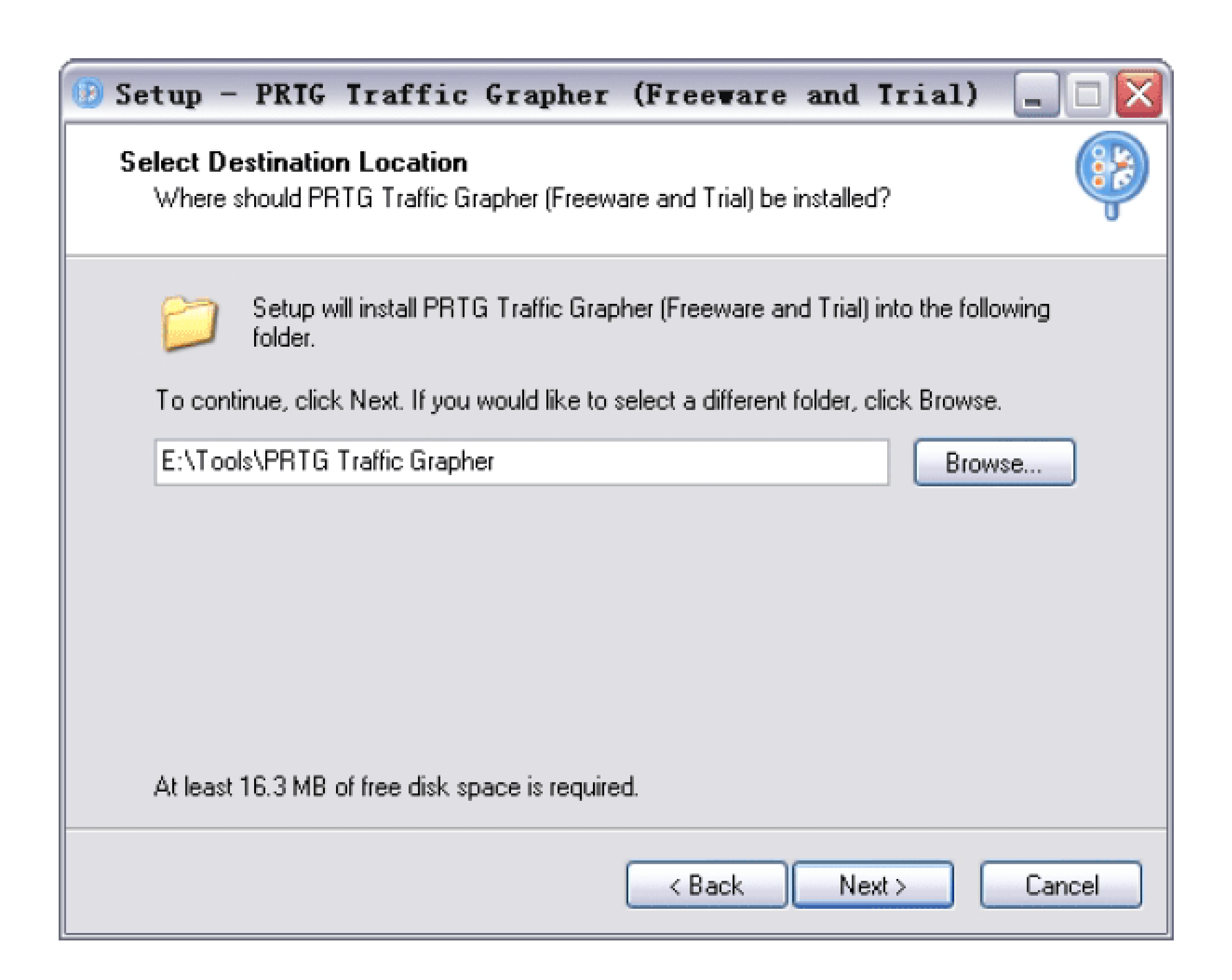


图 9-4　选择安装路径

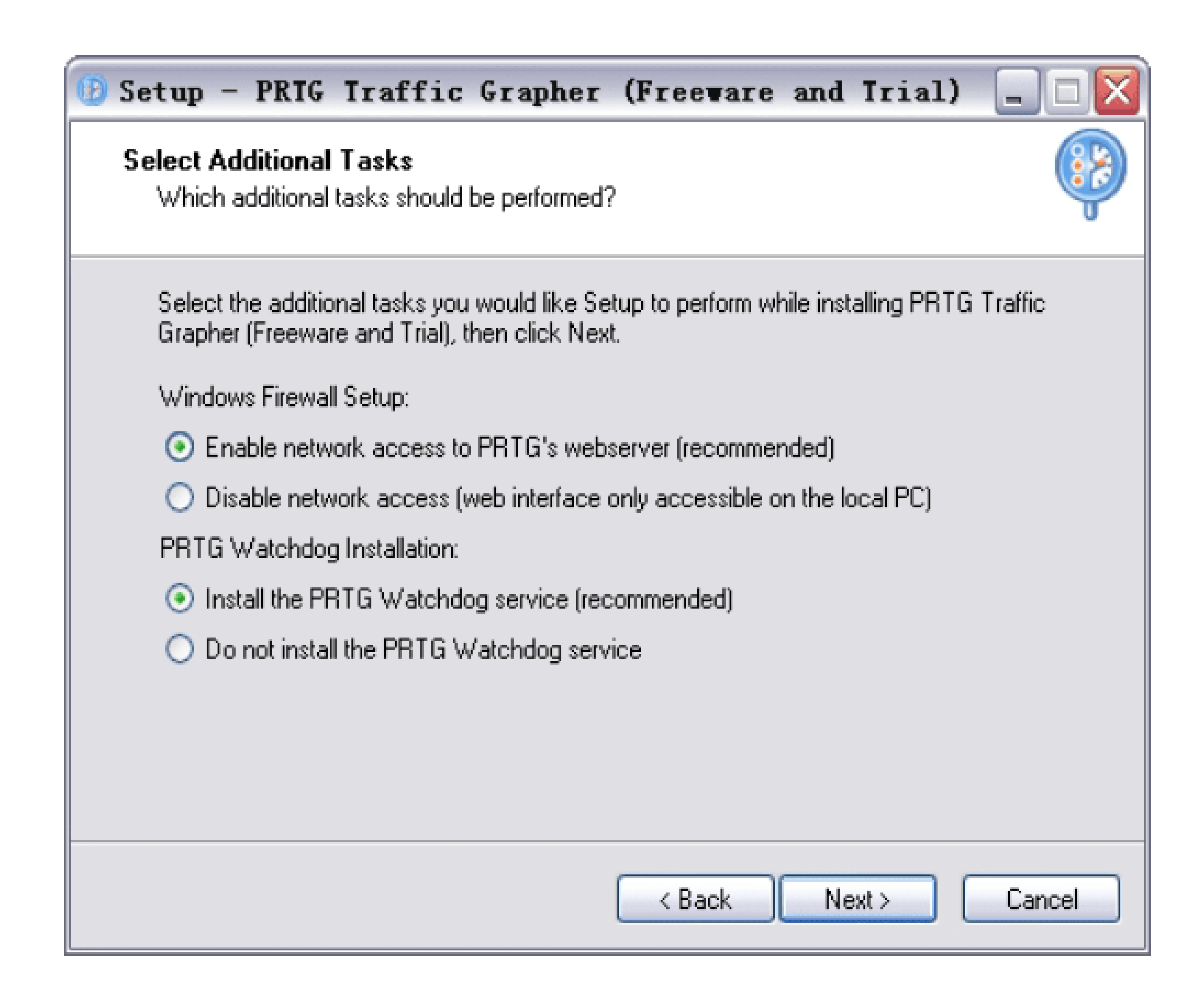


图 9-5　安装设置界面

（4）单击 Next 按钮开始程序的安装，直到安装结束，如图 9-6 所示。

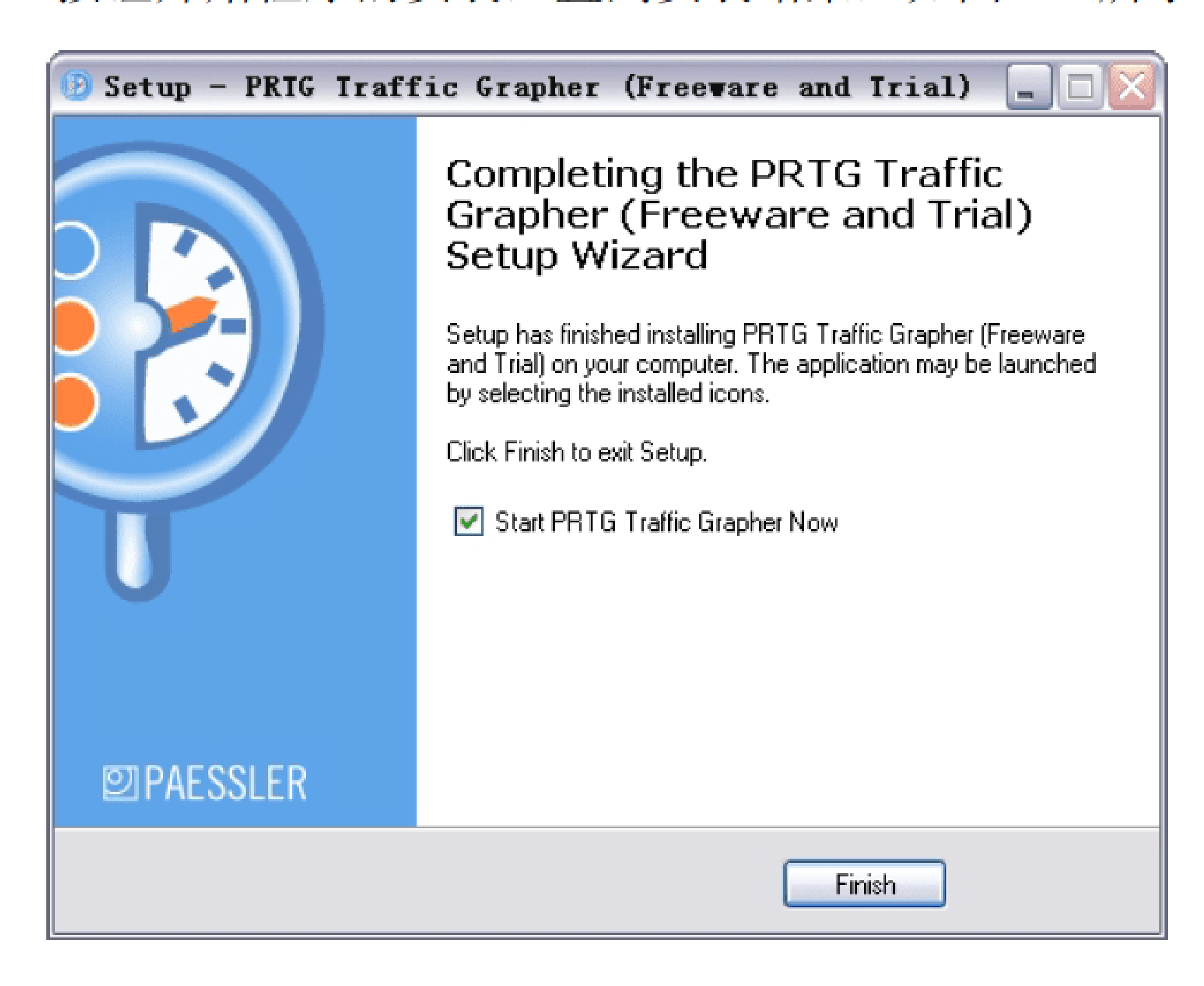


图 9-6　PRTG 安装完毕

（5）安装完毕后，在未对 PRTG 做监测节点配置的运行界面如图 9-7 所示。

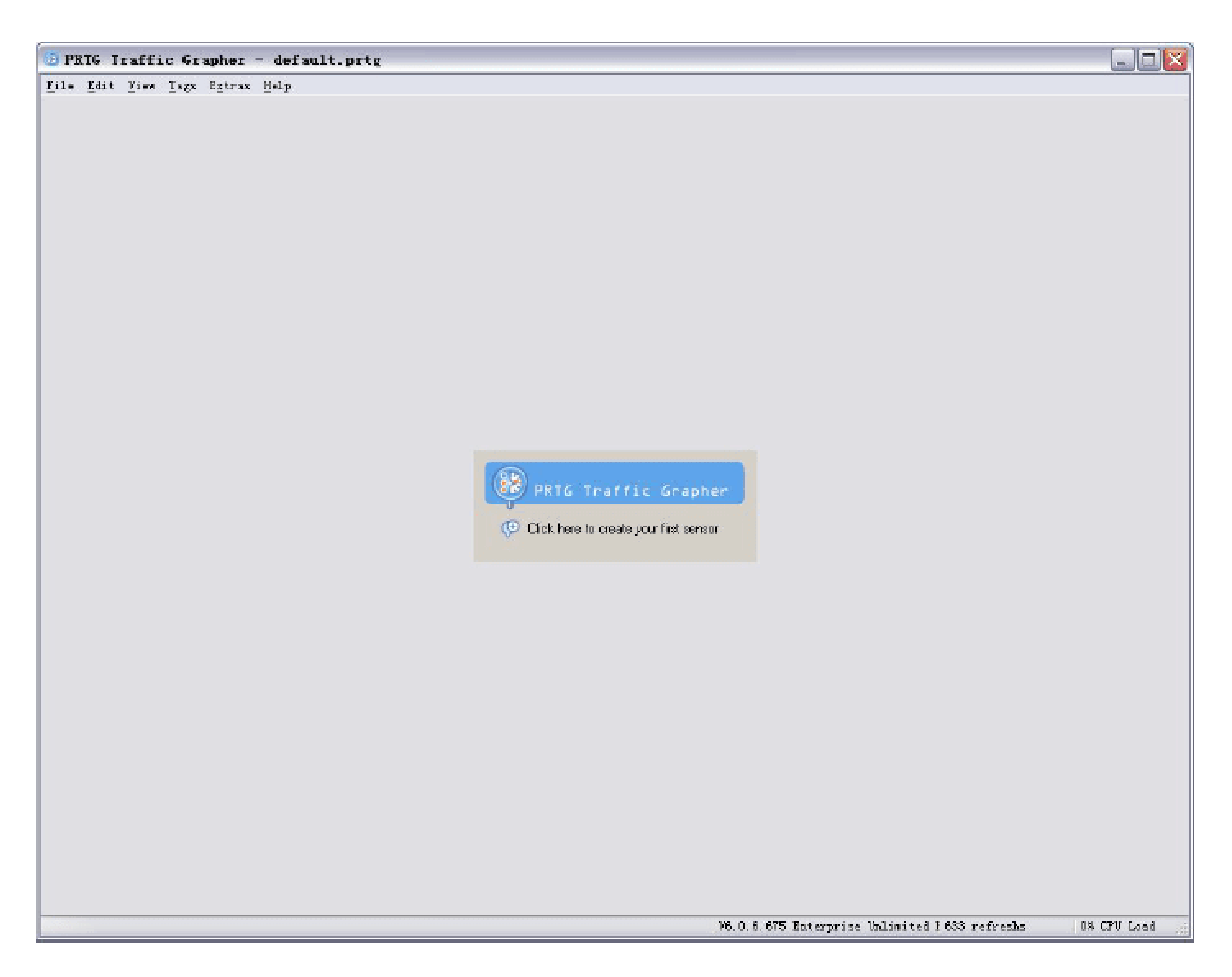


图 9-7　PRTG 运行界面

9.2 SNMP helper 简介及安装

Paessler SNMP Helper 是 PRTG 在采集 Windows 操作系统信息时使用的 SNMP 辅助工具。使用 PRTG 能够搜集 Windows 服务器和工作站更深层的性能信息，甚至多达几千个系

统参数和性能指标。

SNMP helper 的版本包括 Pro Edition 和 Pro Extensions 两个版本。

Pro Edition 的版本为服务器和工作站添加了超过 2000 个 Windows 性能指标，可以在 Windows 2000/XP/2003 系统上运行，能够监控系统中的 2137 个统计对象。

Pro Extensions 版本在监控 Windows 性能指标外，还支持 MS Exchange Server、MS ISA Server、MS SQL Server 等应用服务的深层监控。可监控的对象有如下几种。

- MS Exchange Server：超过 1700 性能计数器指标；
- MS SQL Server：超过 500 性能计数器指标；
- MS Biztalk Server：32 个性能计数器指标；
- MS ISA Server：149 个性能计数器指标。

注意：使用 SNMP Helper Pro 必须购买授权或申请 30 天免费试用的序列号。

9.2.1 SNMP helper 系统要求

安装 SNMP Helper 要求做如下简单配置：

- 可支持的操作系统为 Windows 2000/XP/2003；
- 要求使用 TCP/IP 网络连接；
- Windows 系统需要安装 SNMP 服务。

9.2.2 SNMP helper 安装

在 PRTG 安装完成的存放目录已经包含了 SNMPHelper 的安装程序。在 Windows XP 操作系统中，选择安装程序 Paessler SNMP Helper Setup.exe，开始安装 SNMP Helper，如图 9-8 所示。

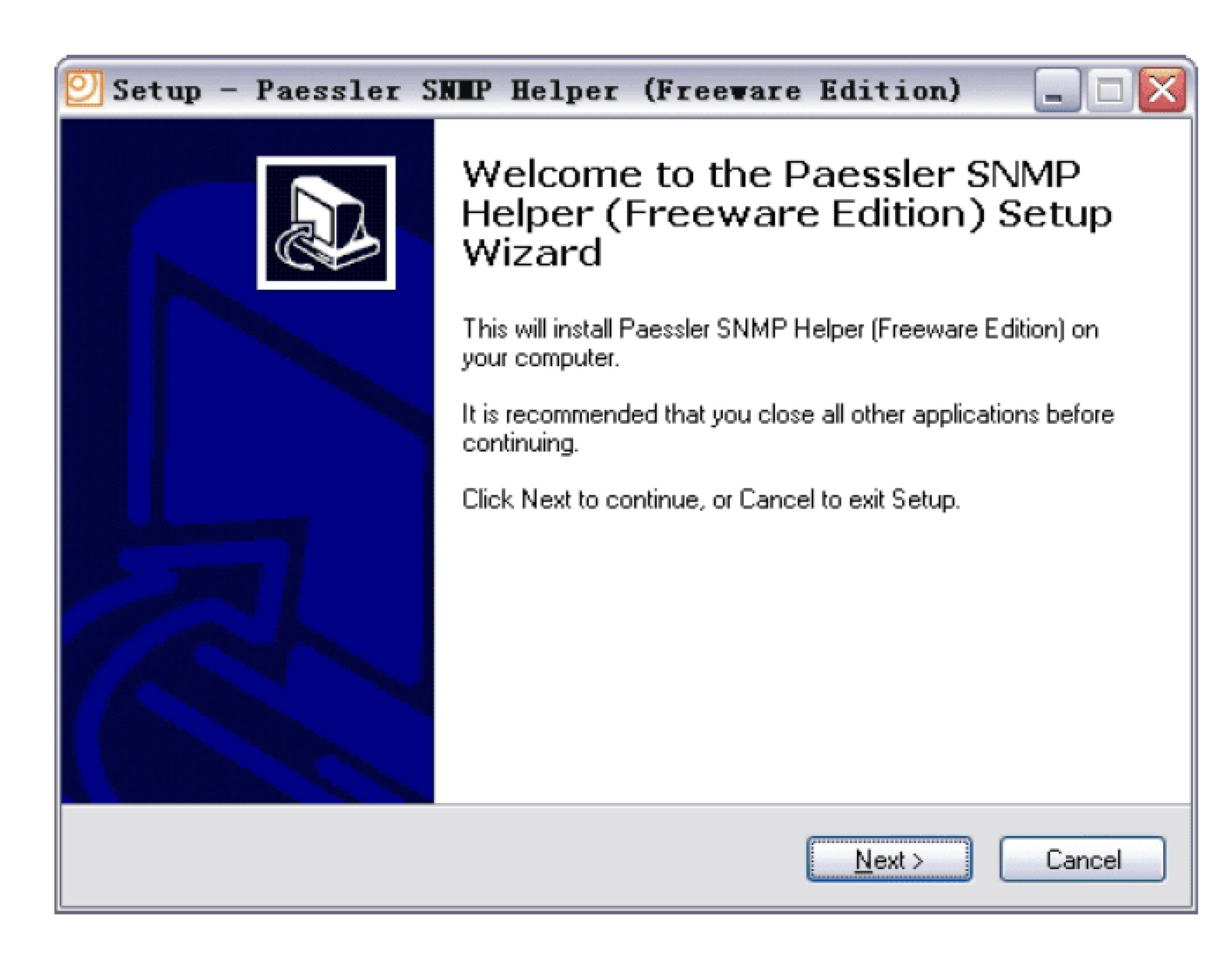


图 9-8 安装 PRTG

单击 Next 按钮进入安装目录的选择，如图 9-9 所示。

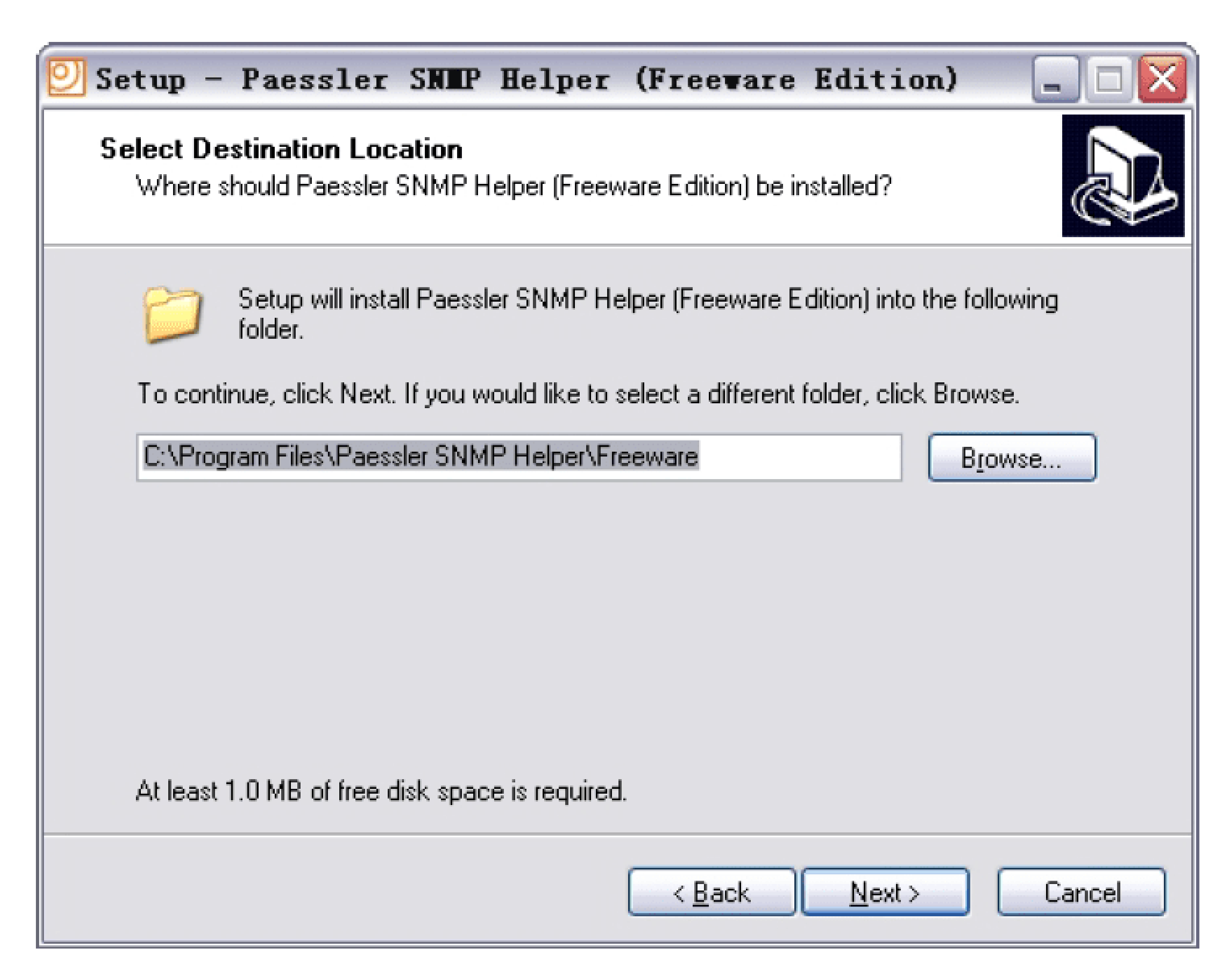


图 9-9　选择 SNMP Helper 安装目录

选择路径后进入下一步，即开始安装 SNMP Helper。安装完成后如图 9-10 所示。

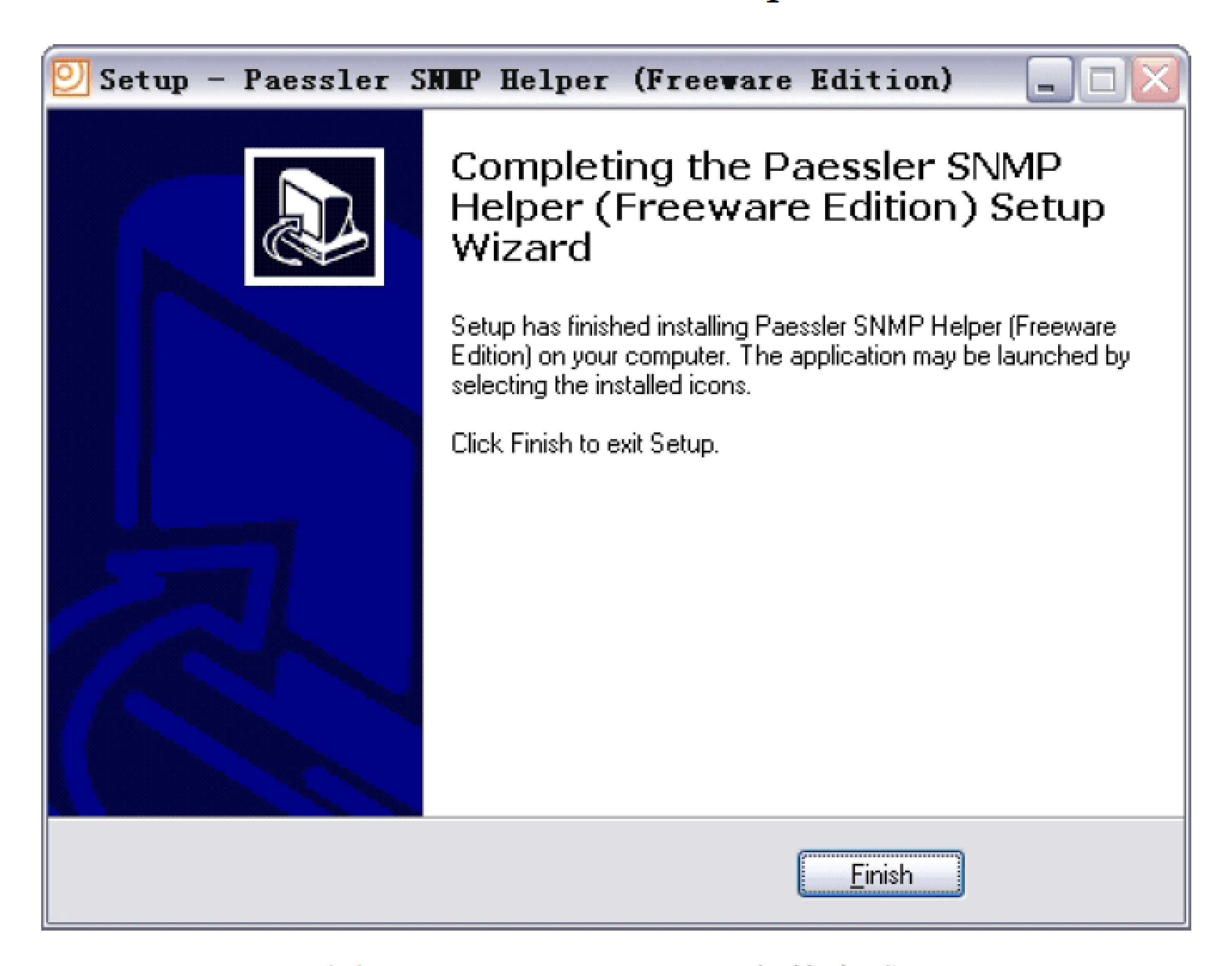


图 9-10　SNMP Helper 安装完成

9.3 PRTG 相关概念简介

9.3.1 SNMP 相关概念回顾

此处对 PRTG 应用涉及的 SNMP 协议及其相关概念做简单回顾，包括 SNMP、MIBs、

OIDs 和 SNMP Community String。

SNMP：该协议标准包含 3 个重要的关键组件，即被管理设备、SNMP 代理和网络管理系统。被管理设备是在网络中包含 SNMP 代理的一个节点，可以是路由器、交换机、计算机或打印机等设备；代理则是设备中的软件模块，负责将信息转换为标准的 SNMP 格式；网络管理系统则是网络监控程序。

MIBs：基础管理信息。MIB 采用有条理、有组织的分级管理体系收集和管理信息，这些信息可以通过 SNMP 协议进行读写访问。

OIDs：在 MIB 分层管理结构中用于识别被管理对象的唯一标示。该标识被定义为树状结构，树的各个层次由不同的组织机构定义。位于组织机构下的私有分支节点，则定义了该组织机构自有产品的管理对象。

SNMP Community string：社区字符串类似于用户身份或密码，用于登录网络设备获取信息的认证。PRTG 向设备发送 SNMP 请求的同时，发送社区字符串。如果字符串正确，设备将响应请求，否则将丢弃请求信息或不应答请求。

9.3.2　PRTG 的 SNMP 工作模式

PRTG 主要通过 SNMP 方式实现流量和带宽的监测，它记录网络设备中流入和流出的数据量，并持续不断地读取设备中流量计数器以获取数值，并统计和分析数据形成图表。如果需要监测其他 SNMP 对象，PRTG 会通过自身的 OID 库或用户自定义的 OID 参数，读取对应设备中指定对象的数值。同时，PRTG 将在数据库中保留历史监测数据。

9.4　查找和添加节点方式详解

9.4.1　通过向导增加监测节点

通过 PRTG 向导添加节点步骤如下：

（1）在 PRTG 主界面中，单击 Click here to add you first sensor 按钮，或选择主菜单中的 Edit | Add Sensor...命令，可打开添加节点向导界面 Add Sensor Wizard，如图 9-11 所示。

（2）选择下一步进入监测方式选择界面，PRTG 共提供了 5 种监测方式，如图 9-12 所示。能够通过 PRTG 所支持的 5 种数据获取方式来监测网络的使用情况。

- SNMP：使用标准 SNMP 访问网络计数器或从支持 SNMP 协议的设备读取数据。
- Packet Sniffing：数据包探测。监测进入\流出本地计算机网卡的所有数据包。
- Netflow Collector：分析思科路由器提供的 NetFlow 数据流方式中的数据包。
- Latency Monitoring：响应时长。通过测量 Ping 操作时长，监测某条数据传输线性能或某设备性能。



图 9-11　添加节点向导



图 9-12　添加节点——选择扫描方式

- Sensor Aggregation：聚合节点。通过添加一个或几个节点的数据集合作为一个新的节点，该节点读取几个节点的信息并生成合计的数据。

以下分别介绍这 5 种方式。

9.4.2　SNMP 监测方式详解

一般用 SNMP 方式监测路由器和交换机的端口带宽利用率。SNMP 设置容易，且占用最低的 CPU 负载和网络带宽，适用于监测包含数百个网络节点的大型网络。

除监测流量参数外，该方式同样适用于监测网络设备和 Windows 系统设备的 CPU 负

载、磁盘利用率、温度及其他参数（根据设备类型而定）。如果监测 Windows 更深入的性能参数，可通过在 Windows 系统中安装 SNMPHelper 代理工具辅助更多参数的获取。

在 Add Sensor Wizard 界面，从 5 种扫描方式中选择 SNMP 扫描方式，并单击 Next 按钮进入 SNMP 扫描方式子项选择界面，如图 9-13 所示。

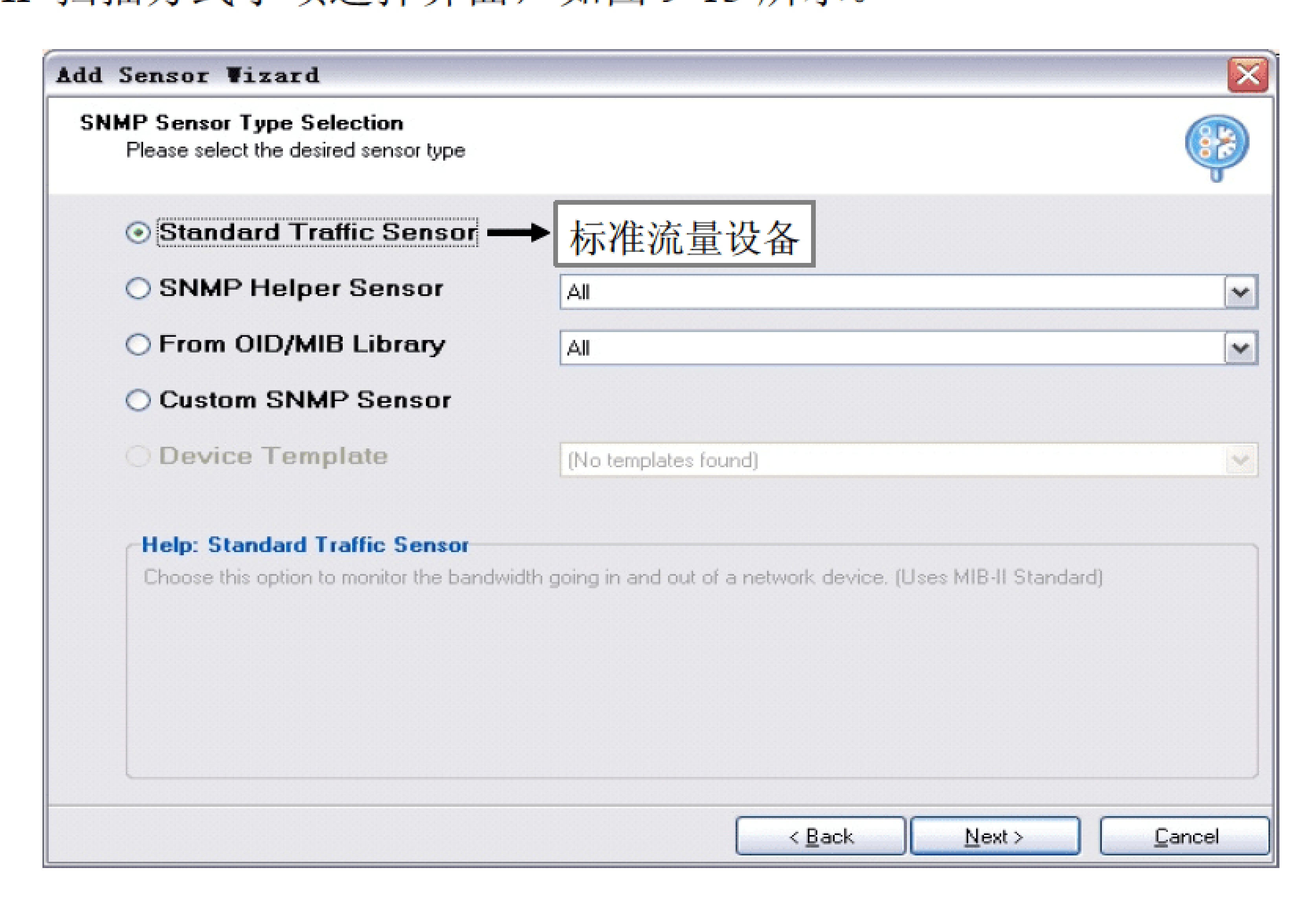


图 9-13 SNMP 扫描方式子项

在 SNMP 方式下，提供了以下 4 种子选项。

（1）Standard Traffic Sensor：标准 SNMP 流量监测方式。通过该方式监测流经指定网络设备的流量情况（使用 MIB-II）。

（2）SNMP Helper Sensor：需要在 Windows XP/2000/2003 操作系统中安装 SNMP Helper 程序，然后根据节点类型来监测性能参数，例如磁盘读写、DHCP 服务请求、邮件服务器等（该选项右边的下拉列表框中列出了各种 PRTG 支持的 SNMP Helper 的版本）。

（3）From OID/MIB Library：PRTG 包含一个普通的 OIDs 数据库，也可以通过导入 MIB 文件建立自定义的 OIDs 库。同样，在选项右边的下拉列表框中列出了已包含的 OID 库。

（4）Custom SNMP Seasor：通过数据监测对象的 OID 用于监测几乎所有的 SNMP 计数器（针对高级用户使用）。

1．Standard Traffic Sensor 标准 SNMP 流量监测方式

首先选择最为常用的 Standard Traffic Sensor 查找方式（见图 9-13），然后进入下一步，打开添加设备对象界面，在该界面中需要输入查找对象的 IP 地址和输入自定义的设备名，如图 9-14 所示。

输入要检测设备的 IP 地址和自定义设备名后，使用默认的 SNMP v1 协议、161 端口和社区字符串 Public（该字符串需要根据对端设备中的实际定义进行设定）。然后单击 Next 按钮进入下一步，即开始通过标准 SNMP 协议查找指定设备。如能正常访问设备，将呈现查找的进度条，如图 9-15 所示。

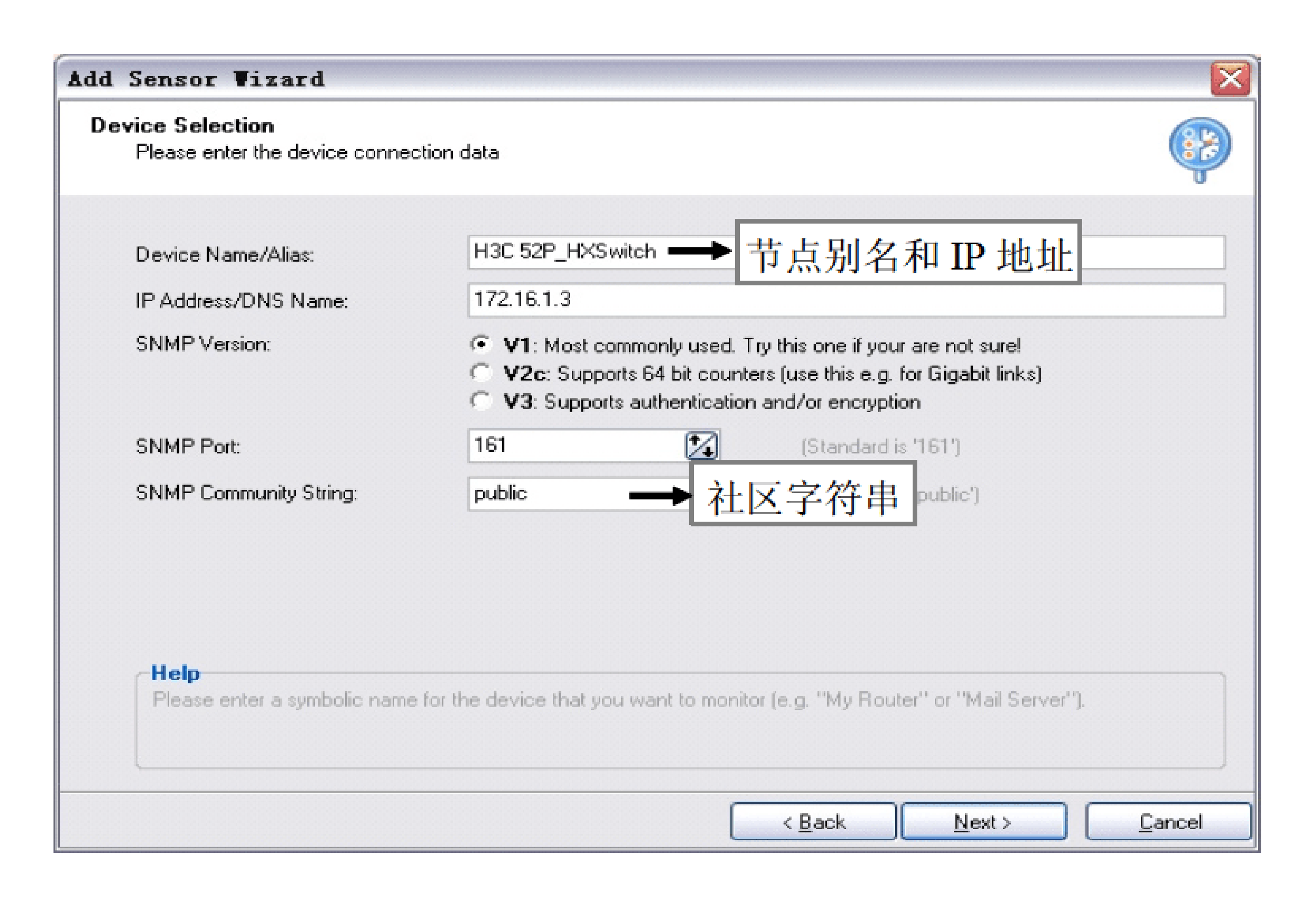


图 9-14　通过标准 SNMP 发现设备

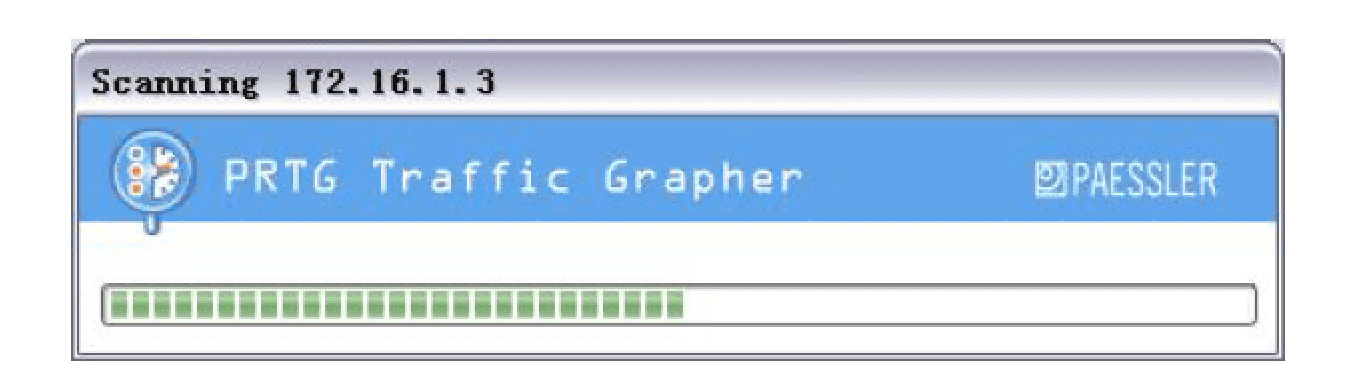


图 9-15　通过 SNMP 方式发现设备

此处查找对象为 H3C 的交换机，找到设备后，将列出交换机各个端口及其连接状态，如图 9-16 所示。

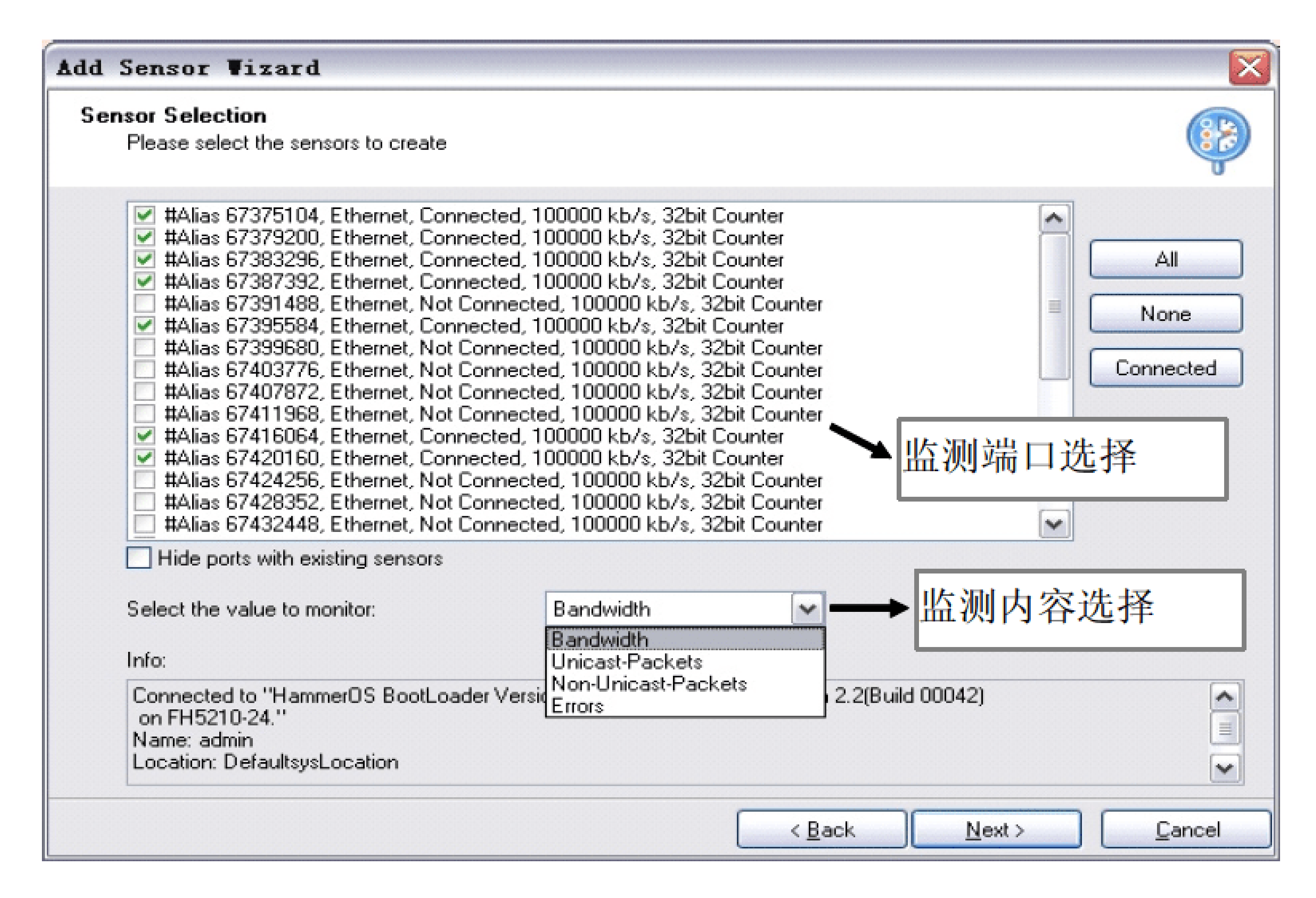


图 9-16　交换机端口选择和监测参数选择

在图 9-16 中，单击 All 按钮，PRTG 将对所有端口进行监测，包括无设备连接的端口；单击 None 按钮，则不监测任何端口；单击 Connected 按钮，则仅监测已连接的端口。也可

以根据需要逐个选择需要监测的端口。在监测参数类型中，提供了 4 种可选项，包括监测端口带宽、非广播数据包、广播数据包和错误数据包。

此处我们选择监测有连接端口的带宽，即选择 Connected 和 Bandwidth 选项之后单击 Next 按钮，进入附加属性设置界面，设置节点分组、采集流量数据的间隔时长和节点类别标识，如图 9-17 所示。

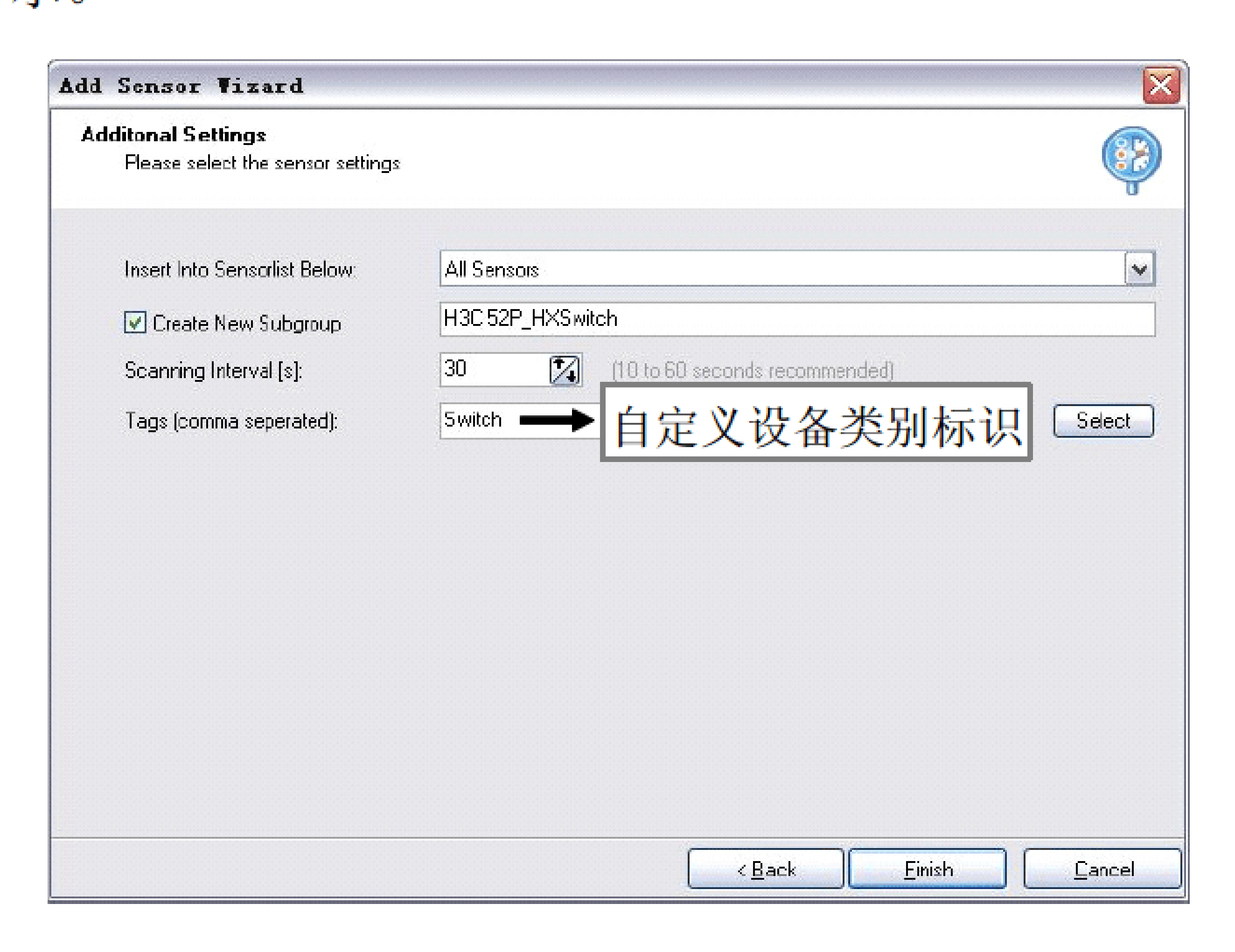


图 9-17 设置附加属性

此时，完成了 SNMP 方式发现并添加监测节点的过程。该节点添加完成后，即可看到监测节点列表及其流量速率，如图 9-18 所示。

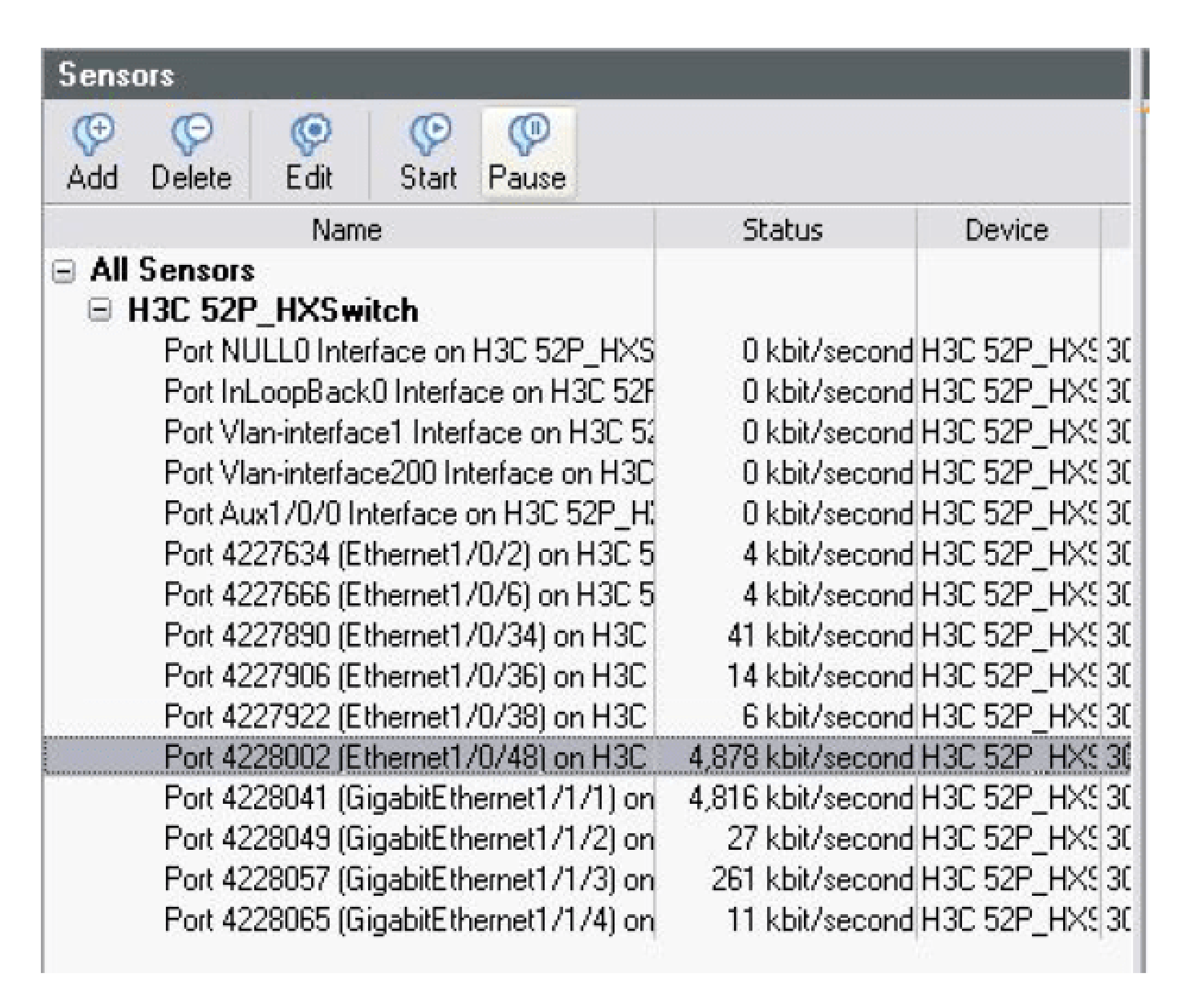


图 9-18 交换机端口流量状态

注意：交换机端口流量以 kbps 为单位，也有以 B/s 为单位的（1Byte=8bits），需要注意区分。

如需查看某一端口的流量曲线图，可选择该端口（例如 Eth1/0/48），在界面右侧将显示流量图，红色曲线为数据流入的速率，绿色曲线是数据流出的速率，采集时间间隔为 30

秒，均以 kbit/s 作为单位，如图 9-19 所示。可以看出，流入的数据峰值约为 1.87Mbps，而流出的数据峰值约为 7.25Mbps。

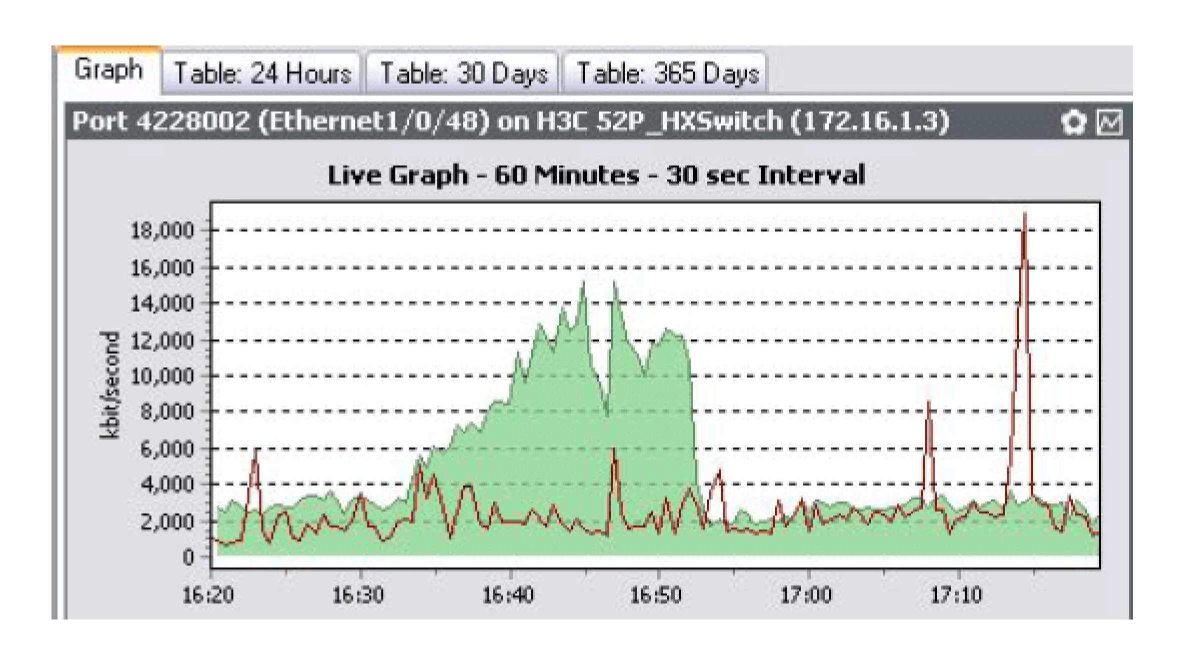


图 9-19　查看交换机某端口流量图

注意：查找过程中，如果弹出 Connection Failed 的报错界面，则表示无法找到设备。该情况有可能是因为网络连接中断、对端设备未开启 SNMP 服务、SNMP 协议版本不匹配或社区字符串不匹配等原因造成的。可按界面提示步骤查找原因。

2. SNMP Helper Sensor 通过 SNMP 代理监测对象

使用 SNMP Helper Sensor 方式监测主机，首先需要在目标主机中开启 SNMP 服务，并安装 SNMP Helper 辅助程序。在 PRTG 安装目录中包含了 SNMP Helper 免费版本的安装程序。安装完成该服务后将自动启动，不需要进行设置。

安装代理程序后，在 SNMP 发现模式下选择 SNMP Helper Sensor 方式，同样输入目标主机的 IP 地址和自定义主机名后，单击 Next 按钮，即可开始查找主机对象。查找结束后将显示通过 SNMP Helper 能够采集的性能参数列表，包括磁盘利用率、内存利用率、网卡流量、进程等参数，如图 9-20 所示。

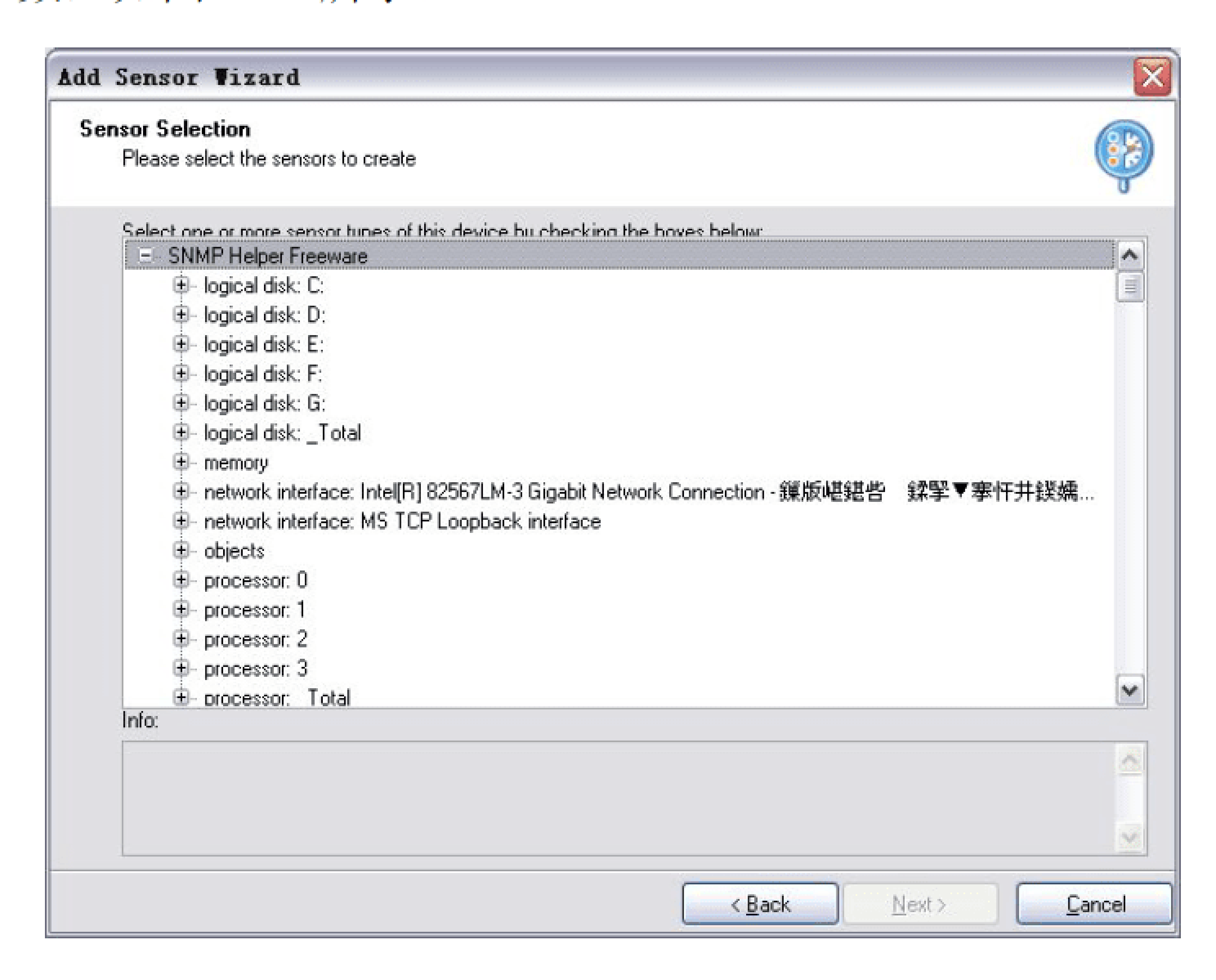


图 9-20　通过 SNMP Helper 获取的计算机性能参数列表

此处选择监测网卡接收数据速率 net bytes received per sec，进入下一步即完成了 SNMP Helper 方式下添加设备的过程。添加完成后，查看该设备最近一小时的流量图可看出，在下午 15：00 左右，本地设备网卡接收数据的流量较大，峰值达到约 550kbps，如图 9-21 所示。

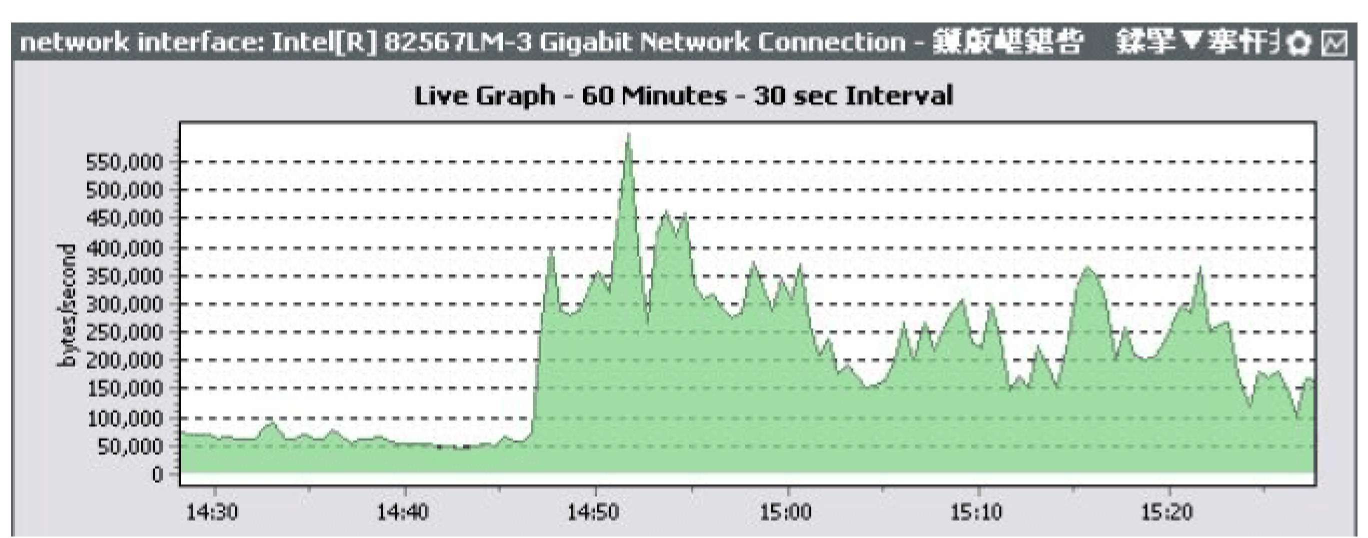


图 9-21　本地网卡接收数据流量

注意：每次新建节点，或者变更某节点设置项后，都需要选择菜单命令 File | Save 进行保存。否则 PRTG 退出后，将不记录任何操作。

3. From OID/MIB Library 监测 OID\MIB 库对象

在 SNMP 发现模式下，选择 From OID/MIB Library 方式，输入目标主机的 IP 地址和自定义主机名进行设备查找后，将显示通过 OIDs 库能够采集的性能参数，包括 CPU 负载、磁盘利用率、物理或虚拟内存利用率、网卡流量，以及通过标准 MIB 库可获取的参数，如图 9-22 所示。

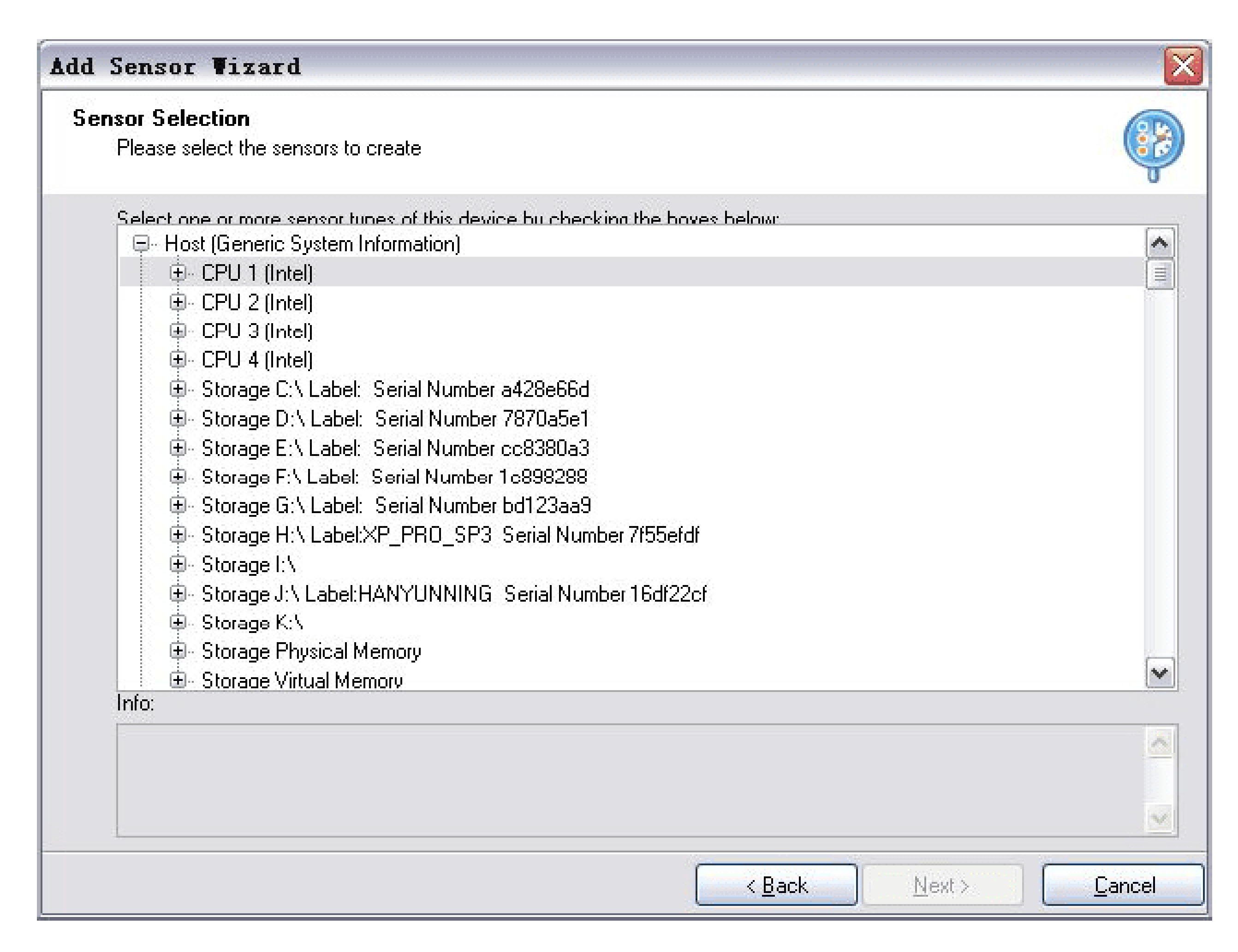


图 9-22　通过 OIDs 库可获取的计算机性能参数列表

此处选择监测 CPU1、CPU2 的负载和物理内存的使用率。进入下一步，完成 OID 方式设备过程。选择该节点可同时查看 3 个监测对象图表，如图 9-23 所示。图 9-23 下方列出了对象使用的曲线颜色。在图 9-23 中，CPU 负载使用左侧的百分比显示，在 18：00 和次日 12：00，计算机为休眠状态，仅占用了 1%～3%的负载。而内存使用右侧的千字节为单位，在休眠期间，耗用了约 700MB 的内存空间用于休眠现场的保存。

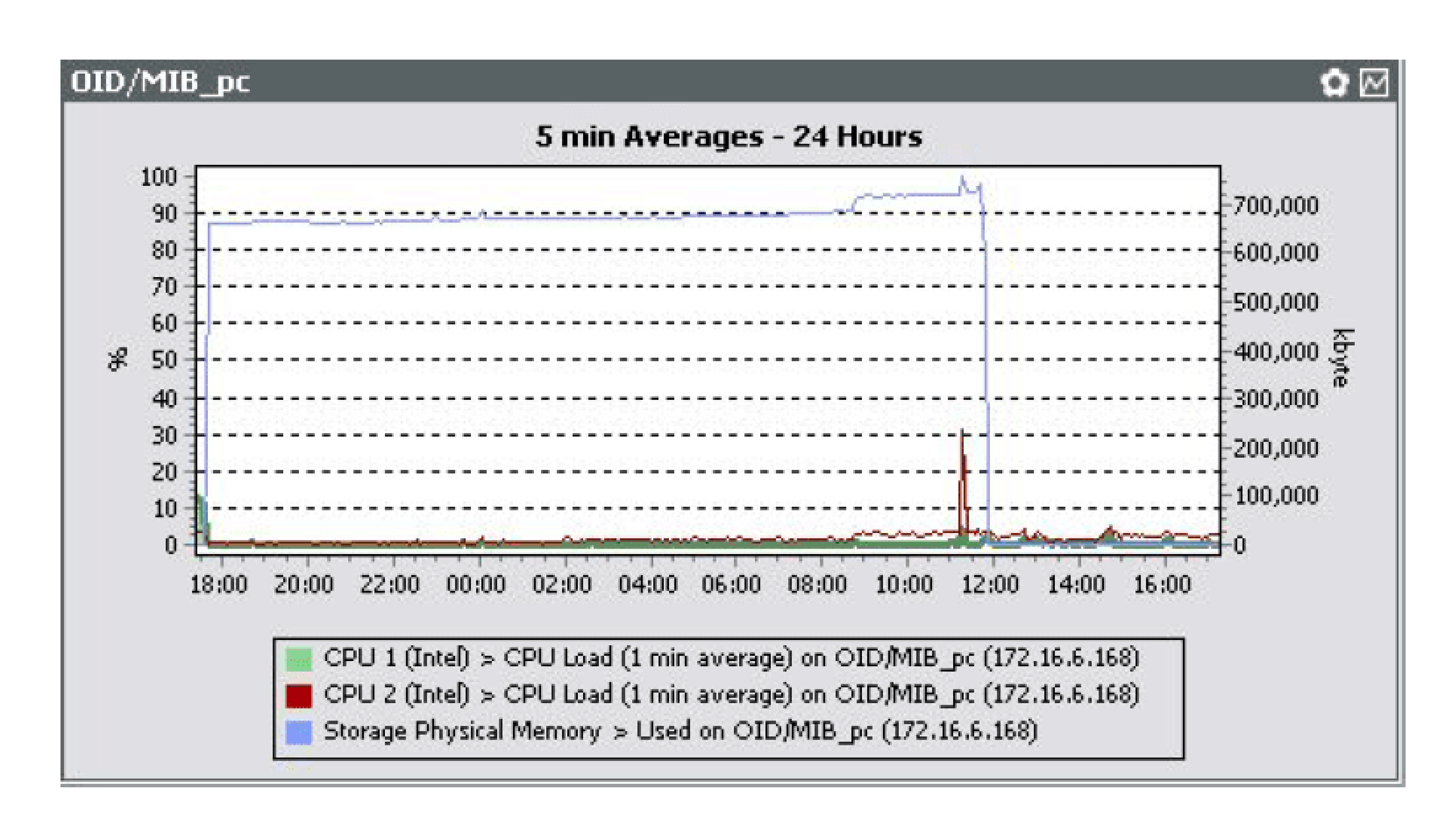


图 9-23　查看 CPU 负载和内存使用率的综合图表

4. Custom SNMP Sensor 监测自定义 OID 对象

使用 Custom SNMP Sensor 方式，需要明确具体监测实例的 OID 数值，该数值可通过 MibBrowser 等工具获取。此处取 OID 对象 iso.org.dod.internet.mgmt.mib-2.icmp.icmpInMsgs（.1.3.6.1.10.1.5.1.0），即获取 ICMP 协议使用过程中流入本机的消息量。MibBrowser 工具获取 OID 标识，如图 9-24 所示。

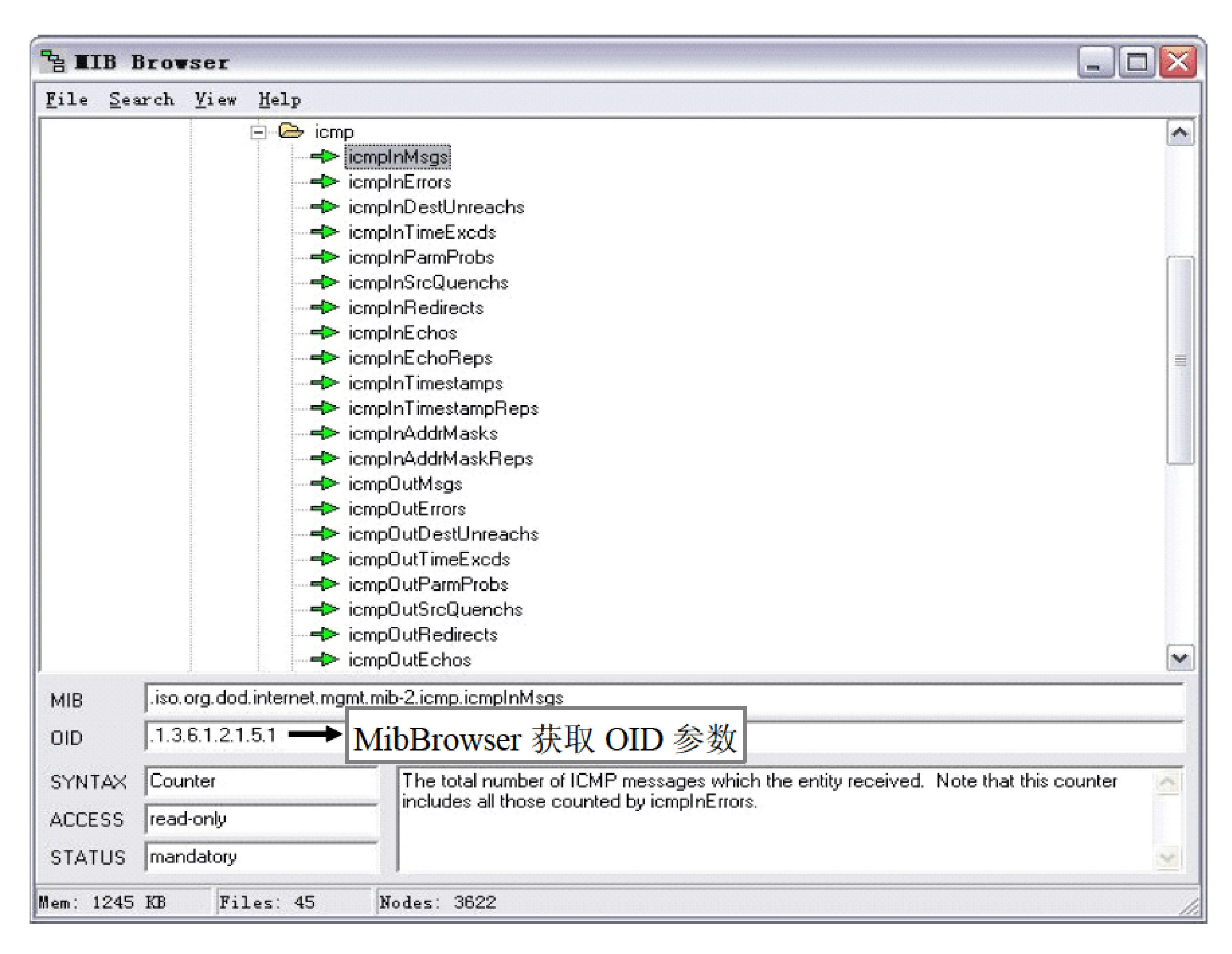


图 9-24　使用 MibBrowser 查看 OID 数值

获取 OID 数值标识后，在 SNMP 发现模式下选择 From OID/MIB Library 方式。设置界面输入 OID 数值后，还需要单击 Test this OID 按钮测试该数值是否正确。如数值正确，将获得该对象的属性或当前参数值，如图 9-25 所示。

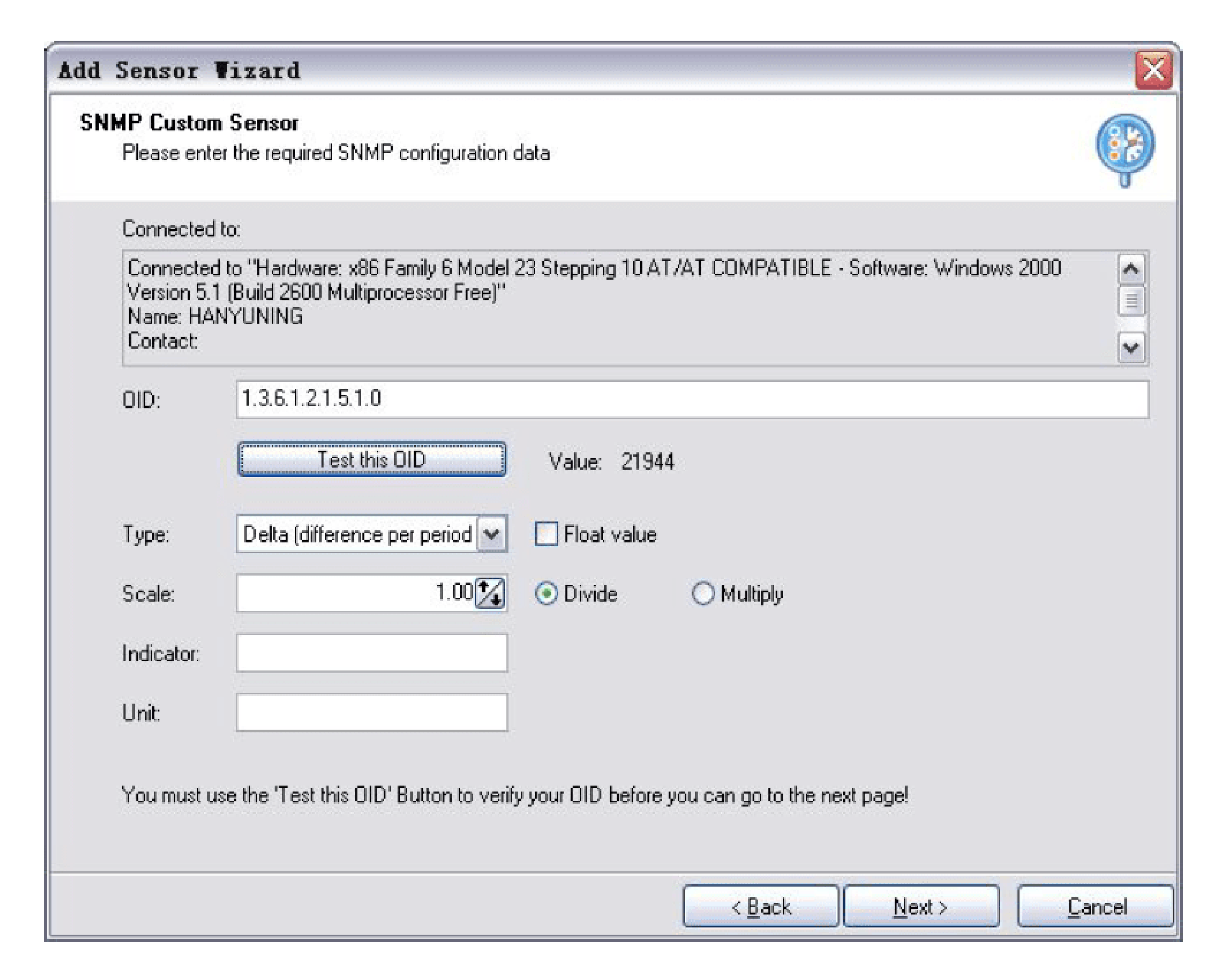


图 9-25　通过输入 OID 可获取的计算机性能参数列表

添加该 OID 对象监测节点后，将在节点列表中看到该节点，如图 9-26 所示。

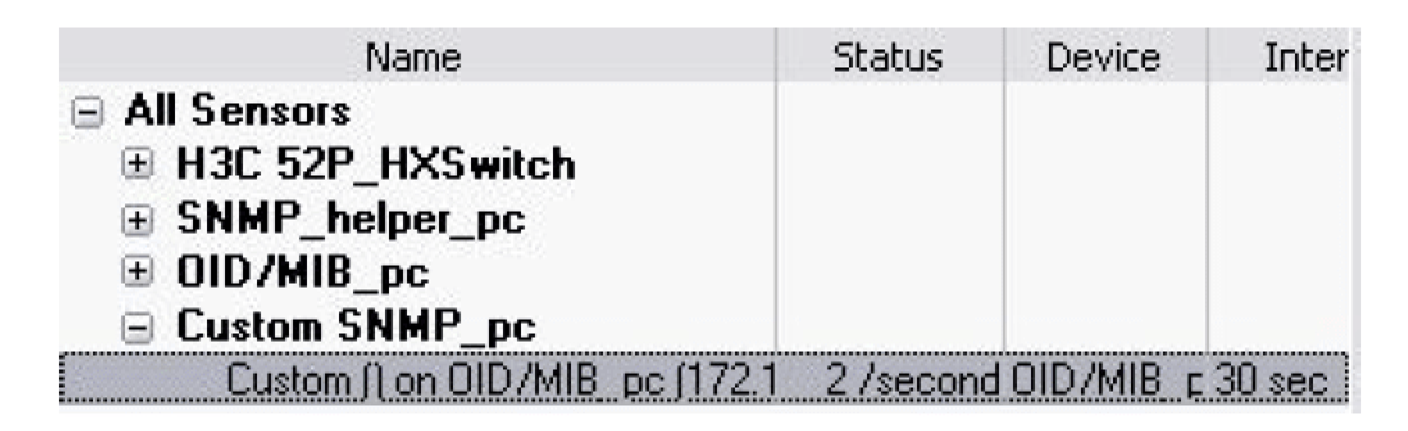


图 9-26　节点列表中包含 OID 方式查找到的节点

查看该 OID 对象的当前 1 小时流量走势图，日常用于交互确认的 ICMP 数据包数量较为稳定。当在 15：55 左右，手动向某网络设备 Ping 命令时，将接收到对端回复的数据包，此时流量图中曲线会有显著的上升，如图 9-27 所示。

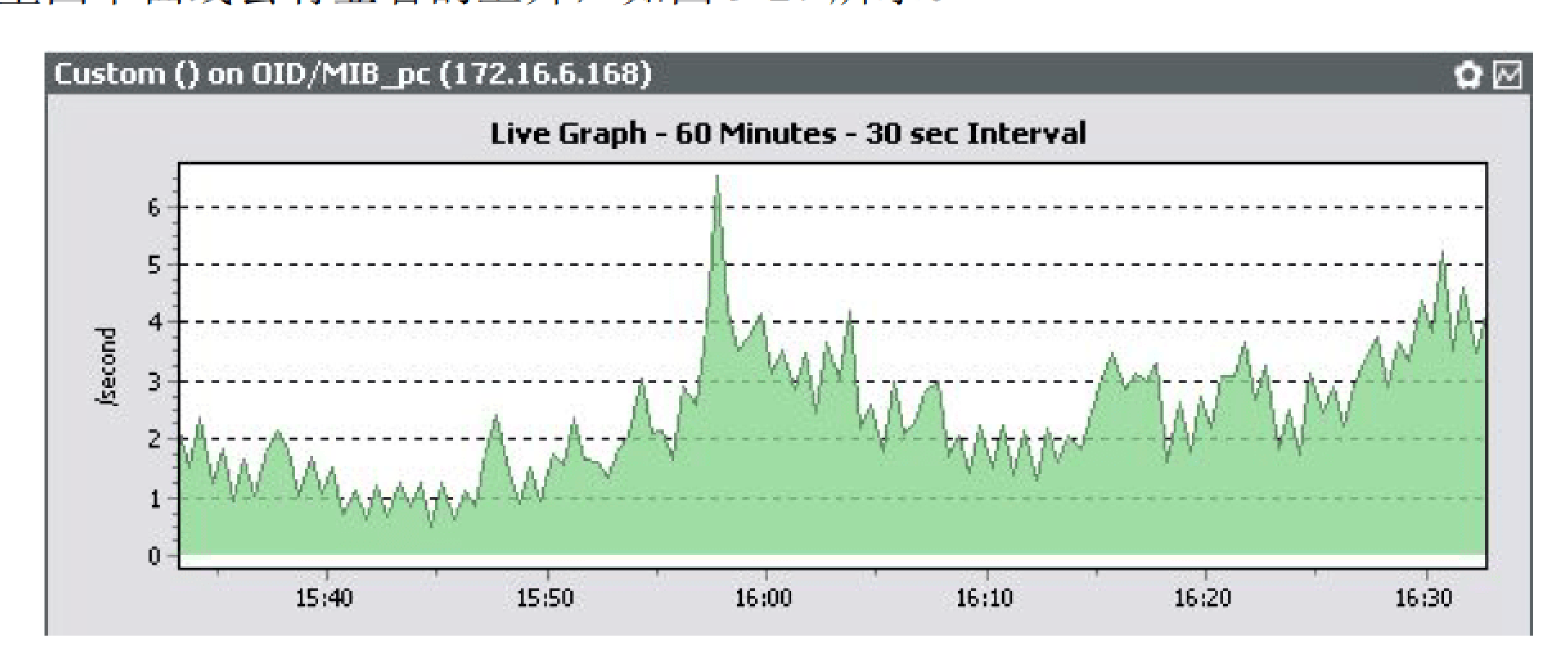


图 9-27　ICMP 协议流入的数据包

9.4.3 Packet Sniffing 数据包探测方式

该方式适用于当网络设备不支持 SNMP 协议，或需要按照网络协议和 IP 地址来详细了解网络带宽使用率的情况。该方式能够探测所有流经（进入\流出）安装了 PRTG 程序的本地网卡数据。

通常，在交换网络中只有特殊的设备才能发送数据到每个网络设备的网卡接口，所以 PRTG 通常并不能监测网络中其他设备的流量信息。如果需要监测网络中的其他设备，则需要使用支持“监测端口”或“端口镜像”的交换机（在思科交换机中，称为 SPAN 技术）。在这种情况下，交换机能够提供流经“监测端口”的所有数据包的拷贝，只要交换机“监测端口”连接了运行 PRTG 的计算机，则 PRTG 能够分析流经该交换机的所有网络信息。

还有另一种方式，就是将 PRTG 安装在所有其他计算机的网关主机上。

注意：数据包探测方式将会占用本机 CPU 最高的负载，适用于流量较小的小型或中型网络。

此处，选择包探测方式监测本地网卡数据流量。设置步骤如下：

（1）在 Add Sensor Wizard 界面中，选择 Packet Sniffing 包探测方式，进入本地计算机网卡选择窗口，在该窗口中列出了可供监测的本地网卡，如图 9-28 所示。

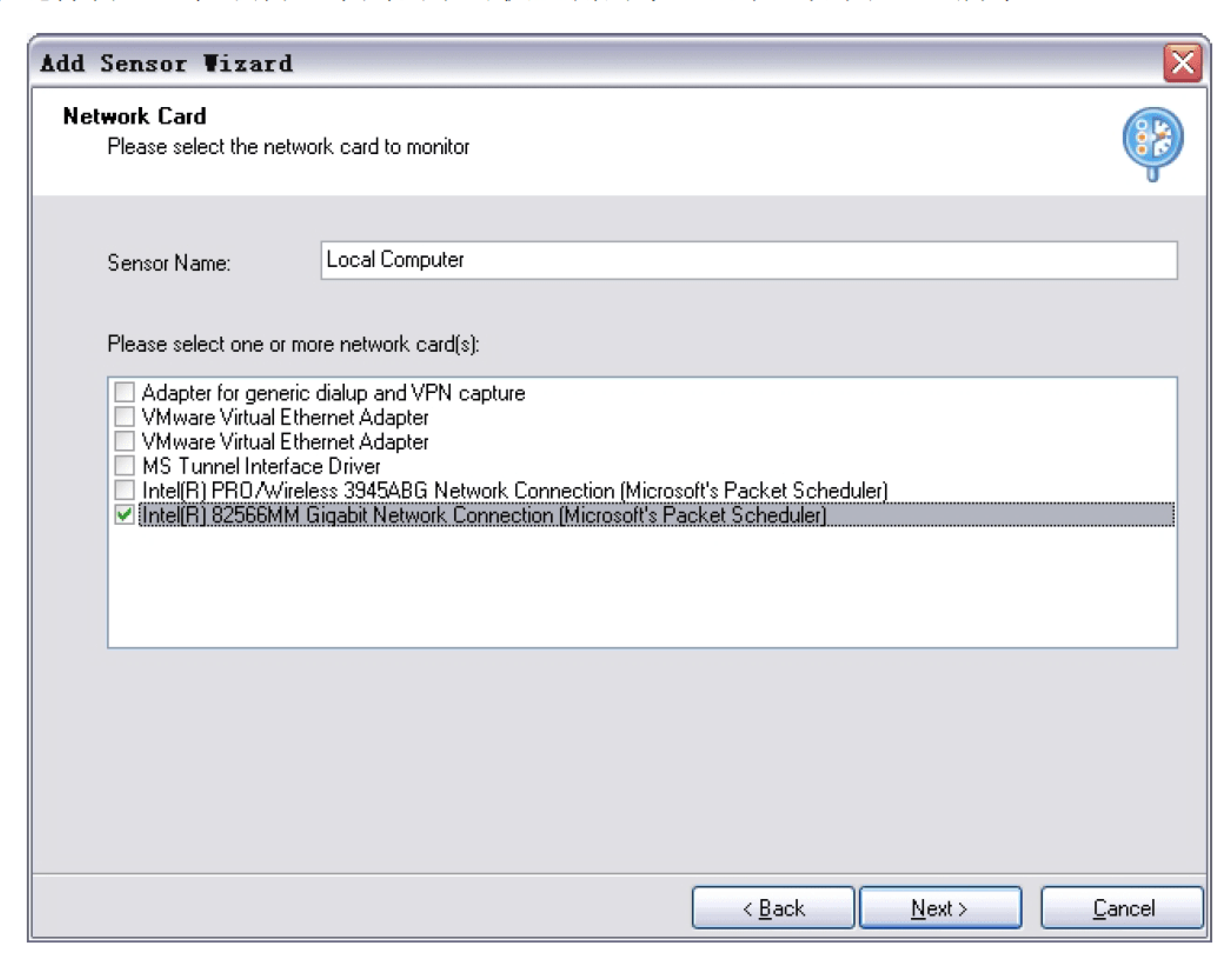


图 9-28　包探测方式，选择要监测的本地网卡

（2）选择接入网络的网卡后，进入下一步进行过滤设置，默认选项为 Monitor All Traffic 及 PRTG 监测所有流经过本机网卡的信息。

如果需要设置过滤选项，则在 PRTG 主界面选择 Filter Traffic | Library 菜单命令可设置过滤规则。过滤方式下，要求至少在 Include Ruleset 中设置一项允许的过滤规则，以及在 Exclude Ruleset 中设置一项排除的过滤规则。允许则表示符合过滤规则的数据包将包含在 PRTG 监测中。反之，符合排除规则的数据包将不被监测。过滤设置界面如图 9-29 所示。

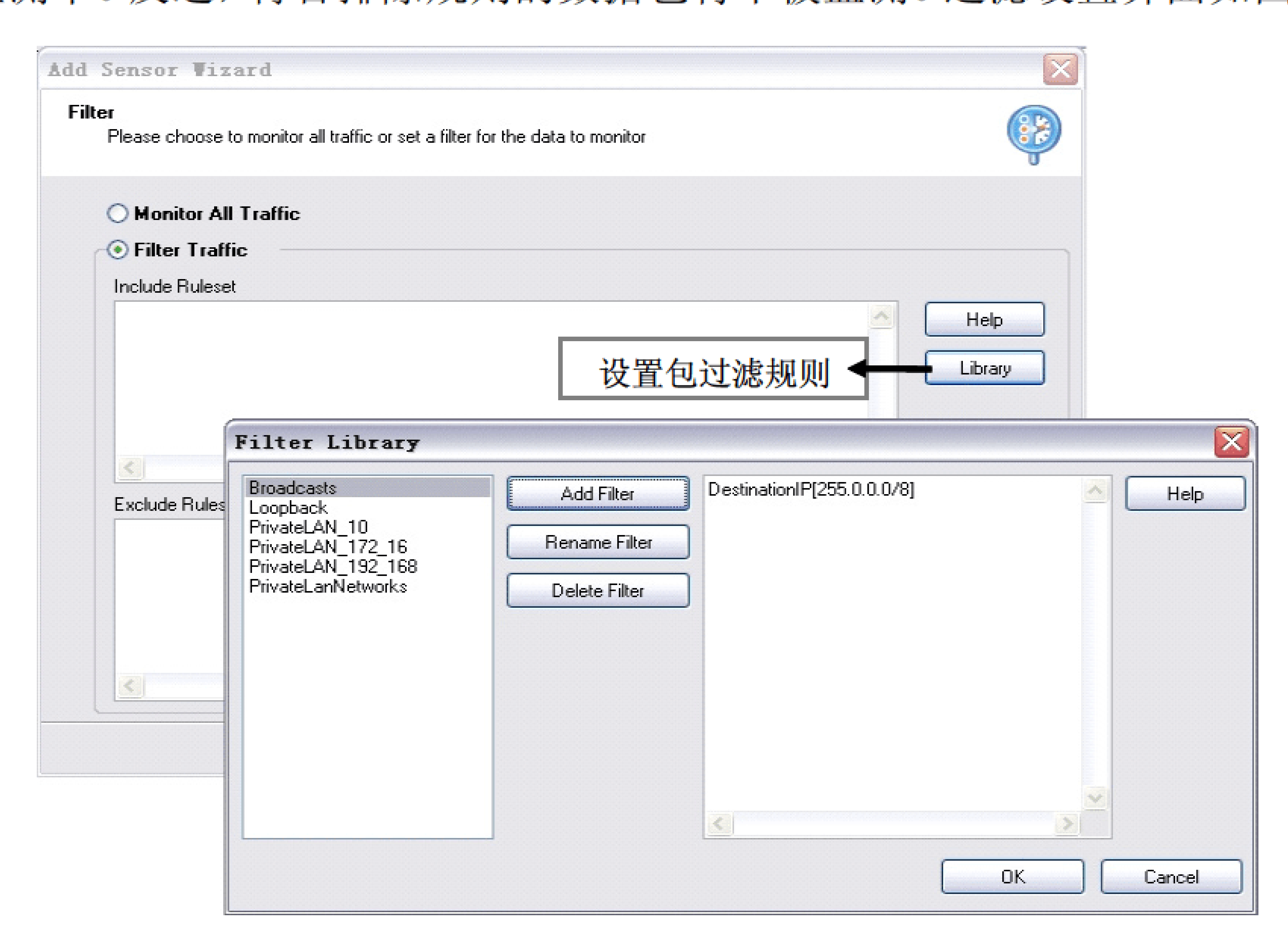


图 9-29　包探测方式：过滤信息选择

（3）如果需要详细了解过滤项目，可单击 Help 按钮查看其详细解释，如图 9-30 所示。

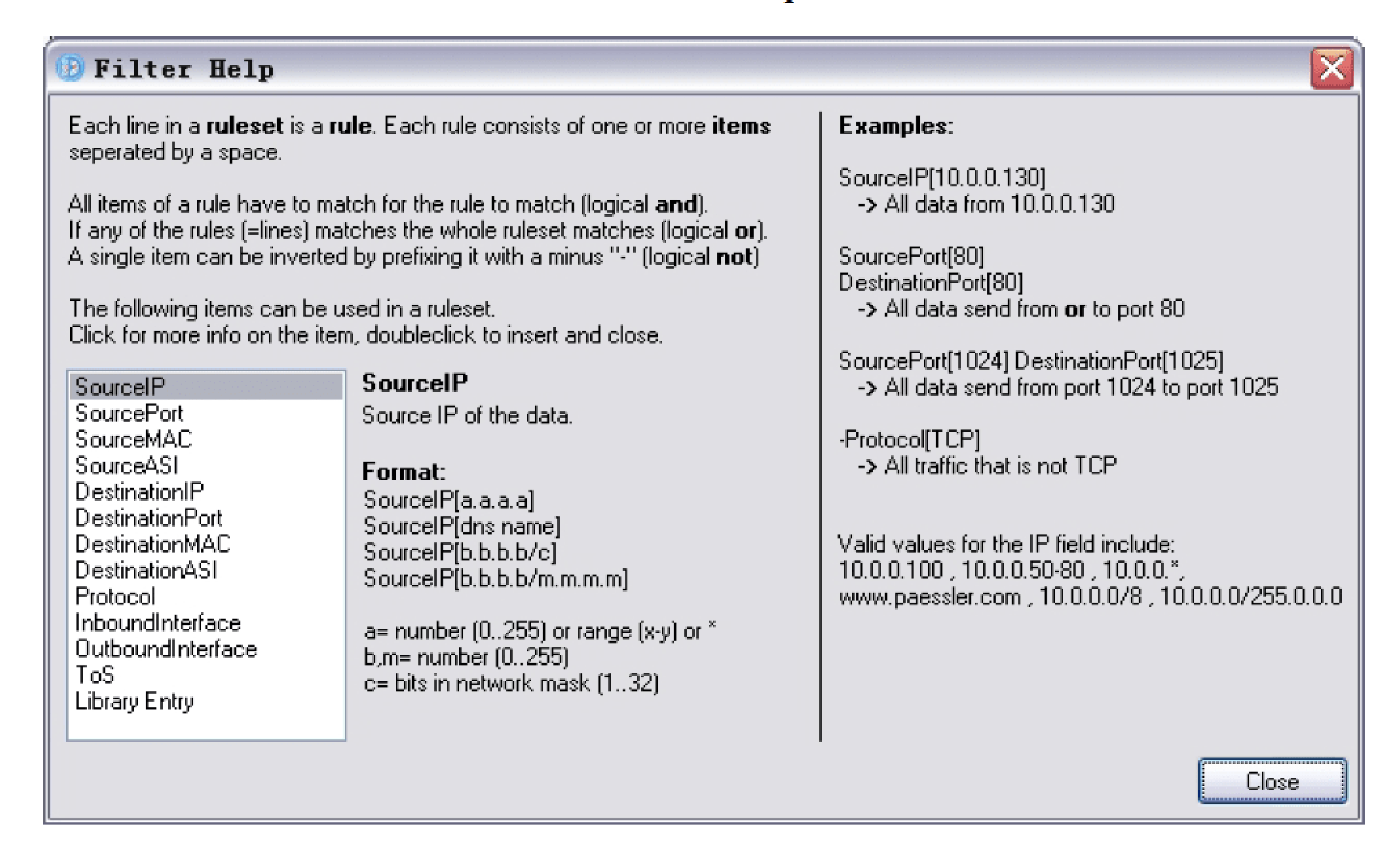


图 9-30　查看过滤选项帮助文件

注意：“允许规则”和“排除规则”，满足允许规则的数据包将被包含在监控范围内，而符合排除规则的数据包则不在监控中。数据包过滤设置较为复杂，推荐较专业的人士使用，通常选择监控所有数据包即可。

（4）选择过滤信息后进入下一步，选择需要监测的协议对象，包括 DNS、FTP、ICMP（Internet 消息控制协议）、HTTP、HTTPS、IMAP（Internet 消息访问协议）、IRC（互联网中继聊天协议）、NETBIOS（网络基本输入/输出系统协议）、POP3（接收邮件协议）、RDP（可靠数据传输协议）、SMPT（邮件发送协议）、SNMP（简单网络管理协议）、SSH（安全外壳协议）、TELNET（远程登录协议）。选择协议对象后（如图 9-31 所示），数据包流量将按所选协议进行分类显示。

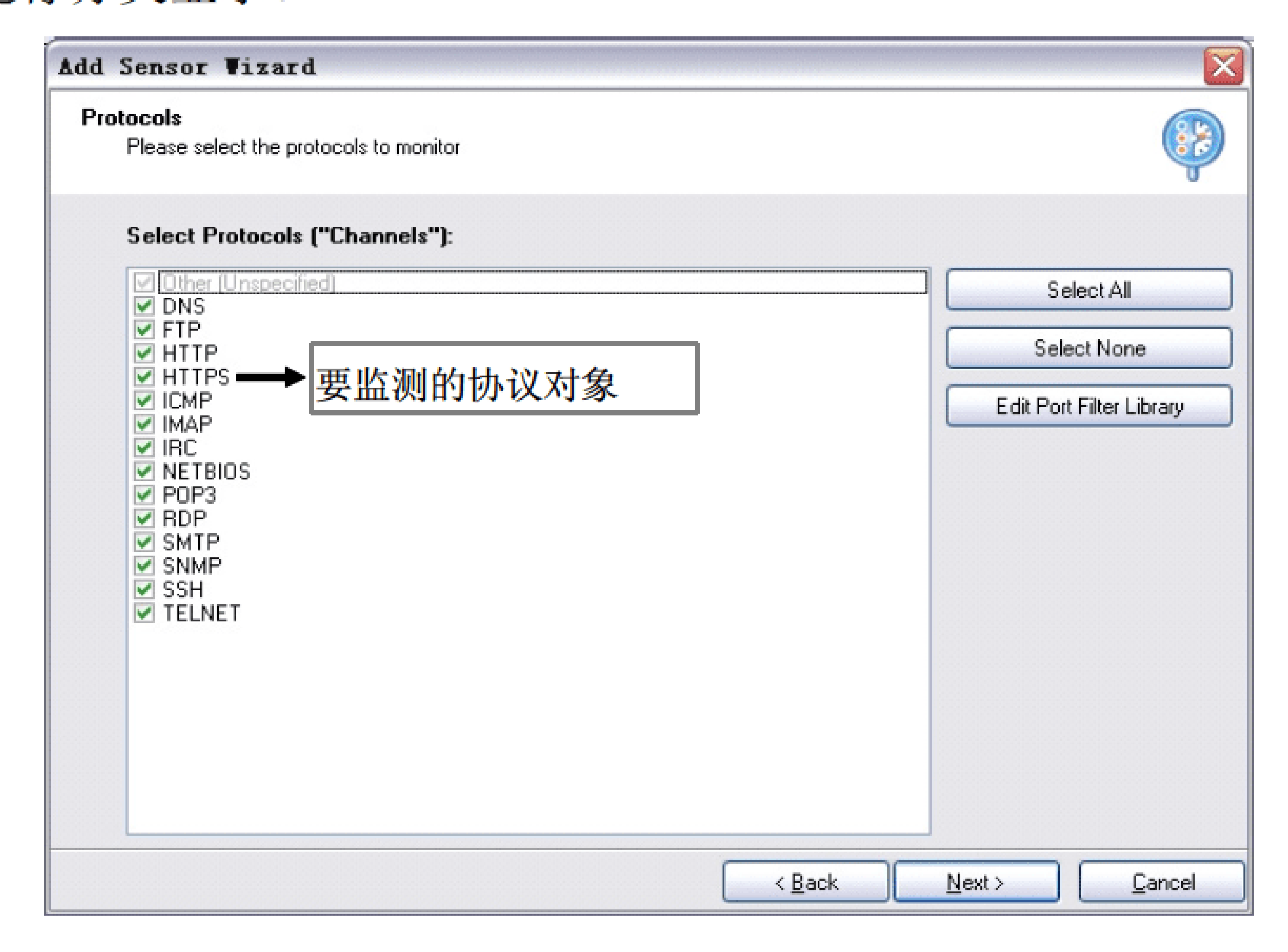


图 9-31　包探测方式：选择要监测协议对象

（5）选择下一步即可完成包探测方式的设置。查看最近 1 小时流量图，可看到流经本地网卡的数据包中，按照各种协议分类显示的流量曲线图，出现峰值的是 HTTP 协议类数据包流量，如图 9-32 所示。

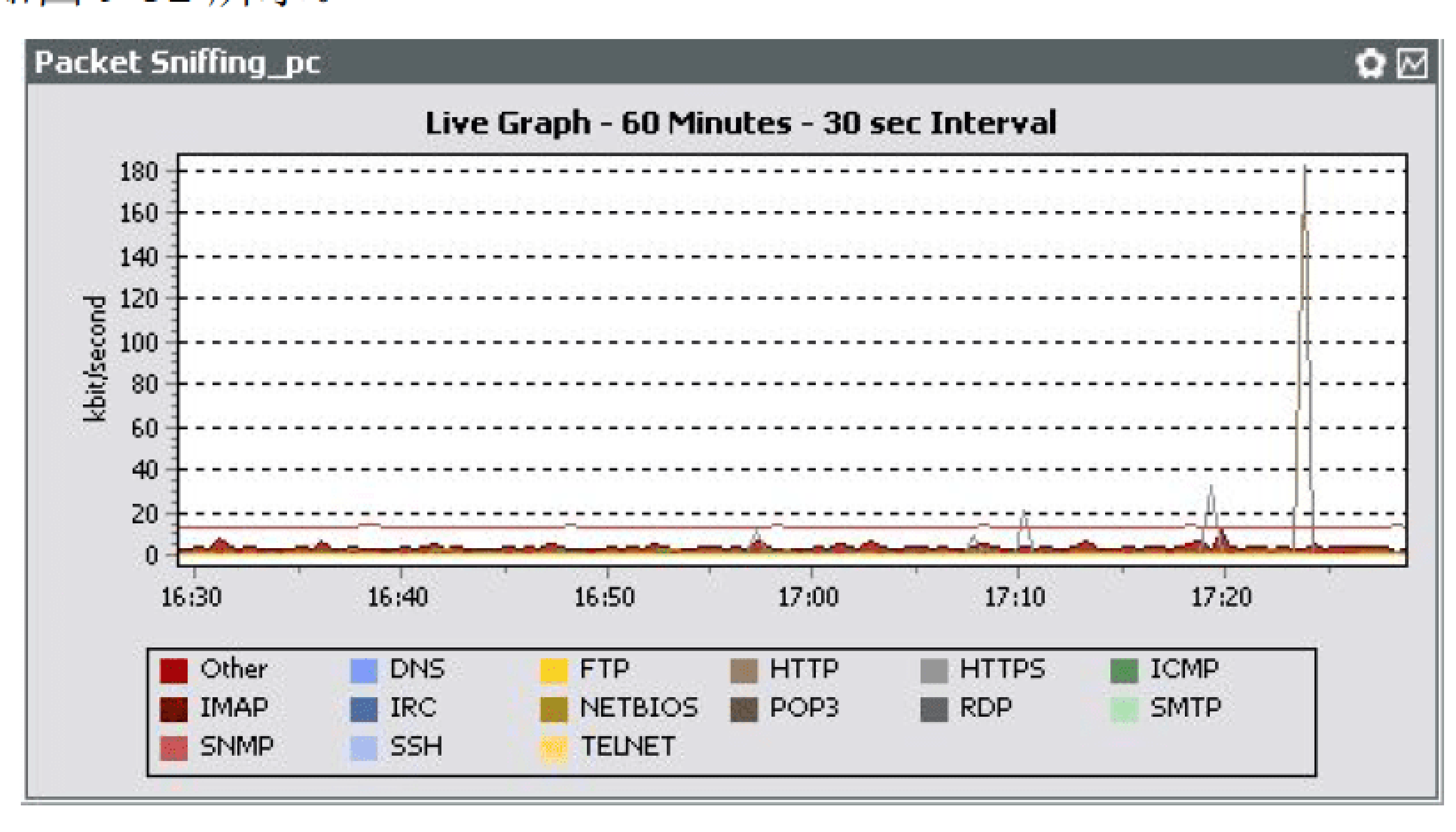


图 9-32　数据包按各类协议划分的流量图

9.4.4 NetFlow Monitoring 数据流监测

1. NetFlow 技术简介

Netflow 技术最早是于 1996 年由思科公司的 Darren Kerr 和 Barry Bruins 开发。它最初用于 Cisco 设备对网络数据交换进行加速，后期发展成为网络中流经路由设备的数据包流量监测和统计分析技术。

NetFlow 技术将网络流量信息记录到设备的高速缓存中，并生成流量统计信息。过期的数据流信息及流量统计数据便组成了 NetFlow 信息。这些信息中包含数据包来源和目的端口、会话传输协议、信息流中的总字节数和数据包数量等。这些信息能够用于网络监控、计费和安全技术。

2. NetFlow 监测方式简介

NetFlow 监测方式仅适用于使用 Cisco 设备的网络。大部分专业的 Cisco 路由器支持该方式用于测量网络带宽。尽管该方式设置最为复杂，但却是最适合于监测大流量网络数据。要使用该方式，还要求更改 Cisco 设备的配置，配置 Cisco 路由器或交换机向安装了 PRTG 的计算机发送数据流，供 PRTG 分析使用。

在 Add Sensor Wizard 界面，选择 Netflow Collector 流监测方式，如图 9-33 所示。

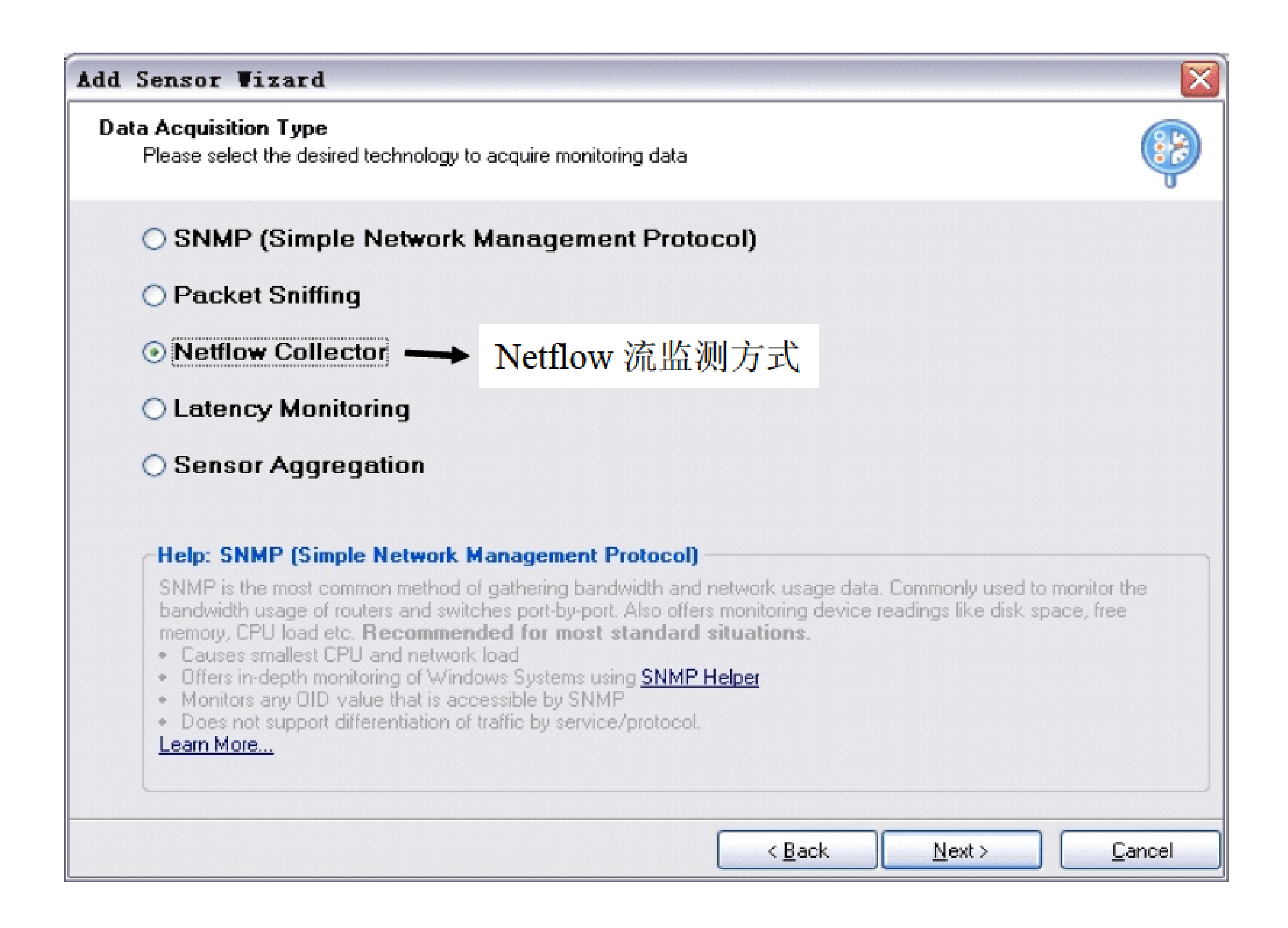


图 9-33　NetFlow 数据流监测方式

单击 Next，进入 NetFlow 对象的选择窗口，选择需要监测的数据流对象后，即完成了 NetFlow 监测方式的设置。

9.4.5 Latency Monitoring 监测响应时长

Latency Monitoring 监测方式下，PRTG 通过向设备发送 ICMP 响应请求（即 Ping 命令），然后记录设备接收到响应信息的时长。在曲线图上，变化幅度较大的 Ping 响应时长，过多的 Ping 丢包可判断某台设备或传输线状态为超负荷。而一条性能稳定的传输线将会显示接近稳定不变的数值。

在 Add Sensor Wizard 界面中，选择 Latency Monitoring 监测方式，然后选择下一步进入设置界面，输入监测对象的设备显示名、IP 地址，选择每次等待应答的时长和每次发送的 Ping 数据包大小（此处选择默认值即可），如图 9-34 所示。

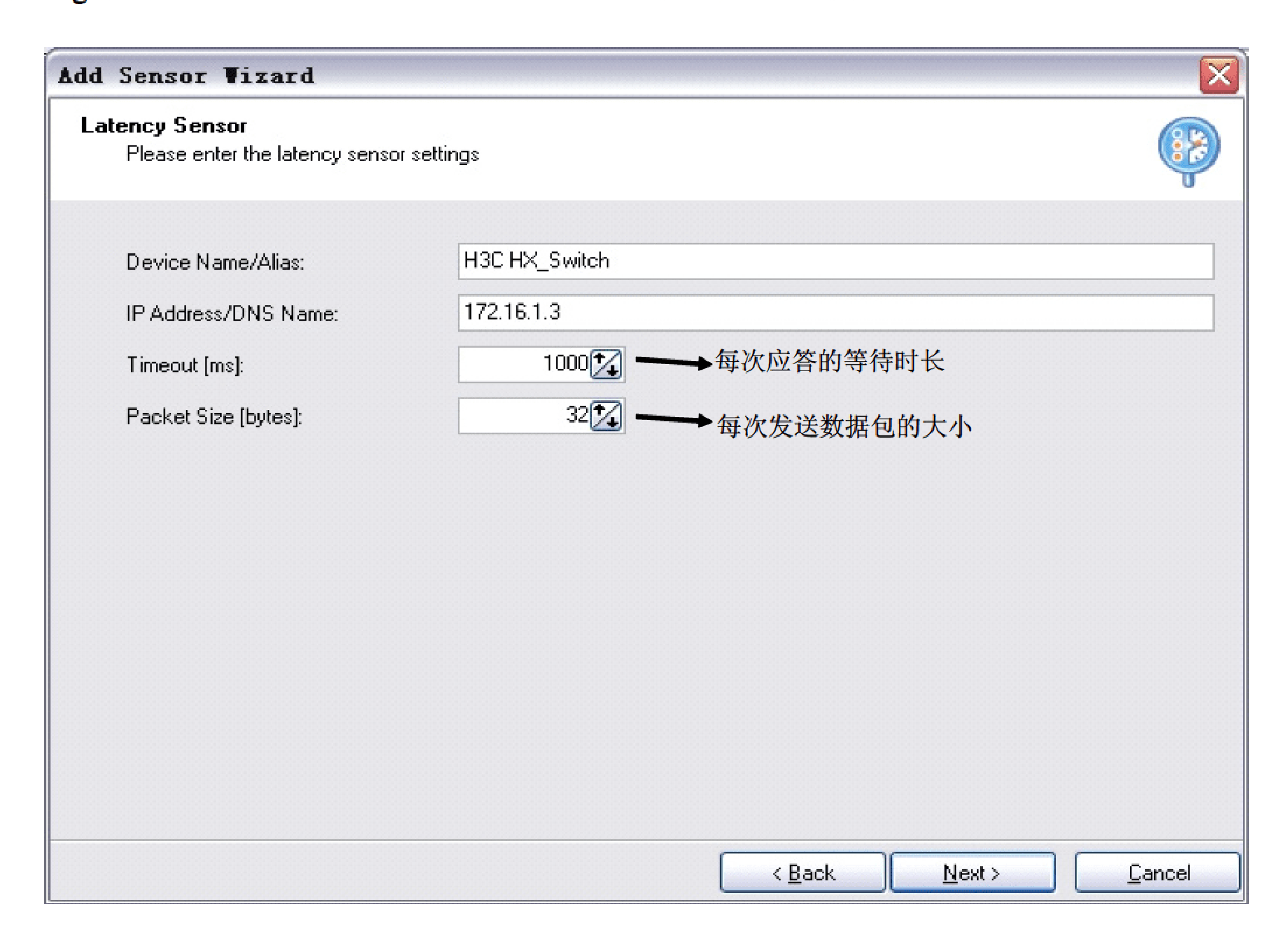


图 9-34　监测响应时长方式设置界面

设置完毕后进入下一步，即可完成监测响应时长方式的设置。查看对应的曲线图可看到 Ping 命令响应迅速和稳定，响应时长在 3～7 毫秒范围内，如图 9-35 所示。

9.4.6 Sensor Aggregation 聚合节点监测方式

在 Sensor Aggregation 方式下，可将几个节点聚合成为一个新节点，新节点将采集各个节点数据的合计值。该方式适用于监测网络中某一系列的端口合计信息。

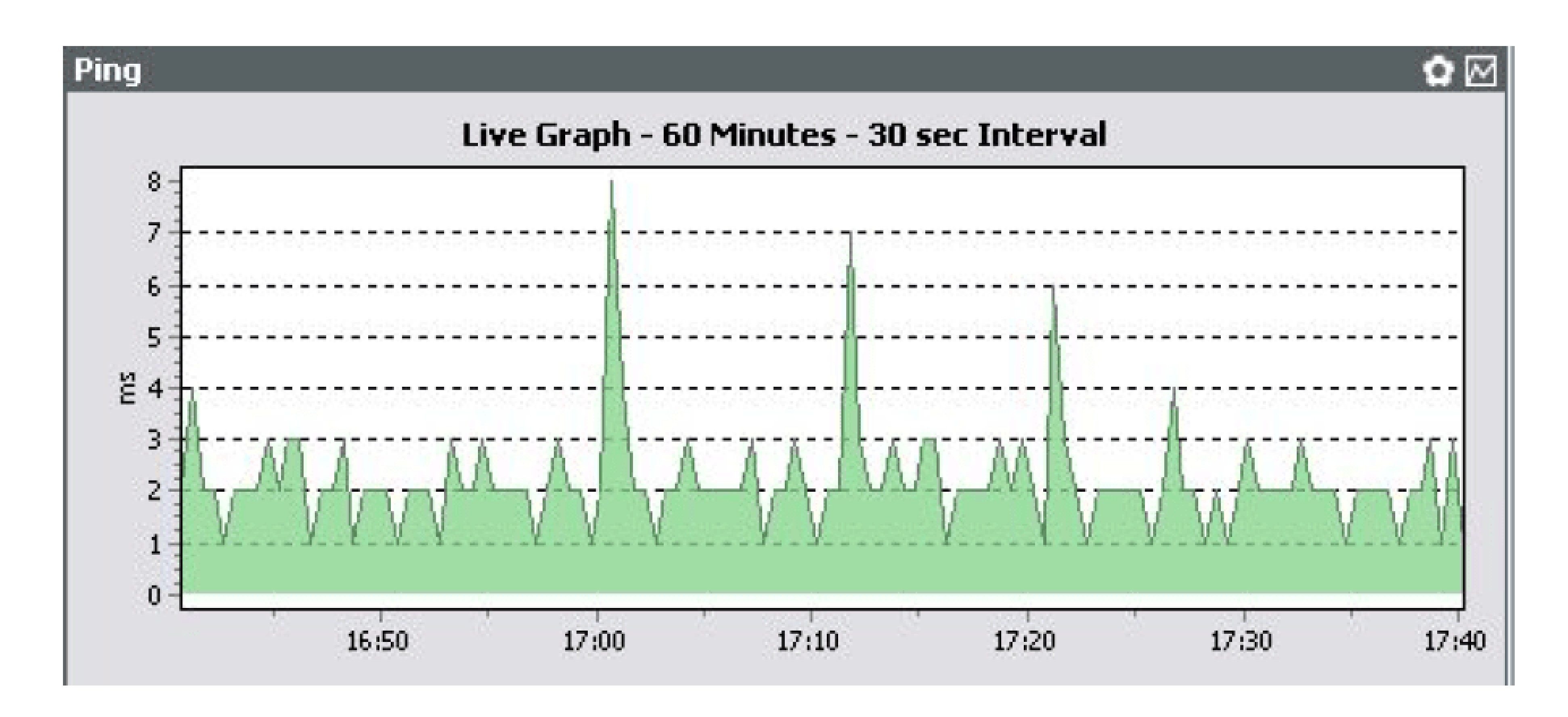


图 9-35　Ping 命令响应时长曲线图

在 Add Sensor Wizard 界面中，选择 Sensor Aggregation 方式，进入节点选择界面，该界面中包含了当前所有已发现的节点，如图 9-36 所示。

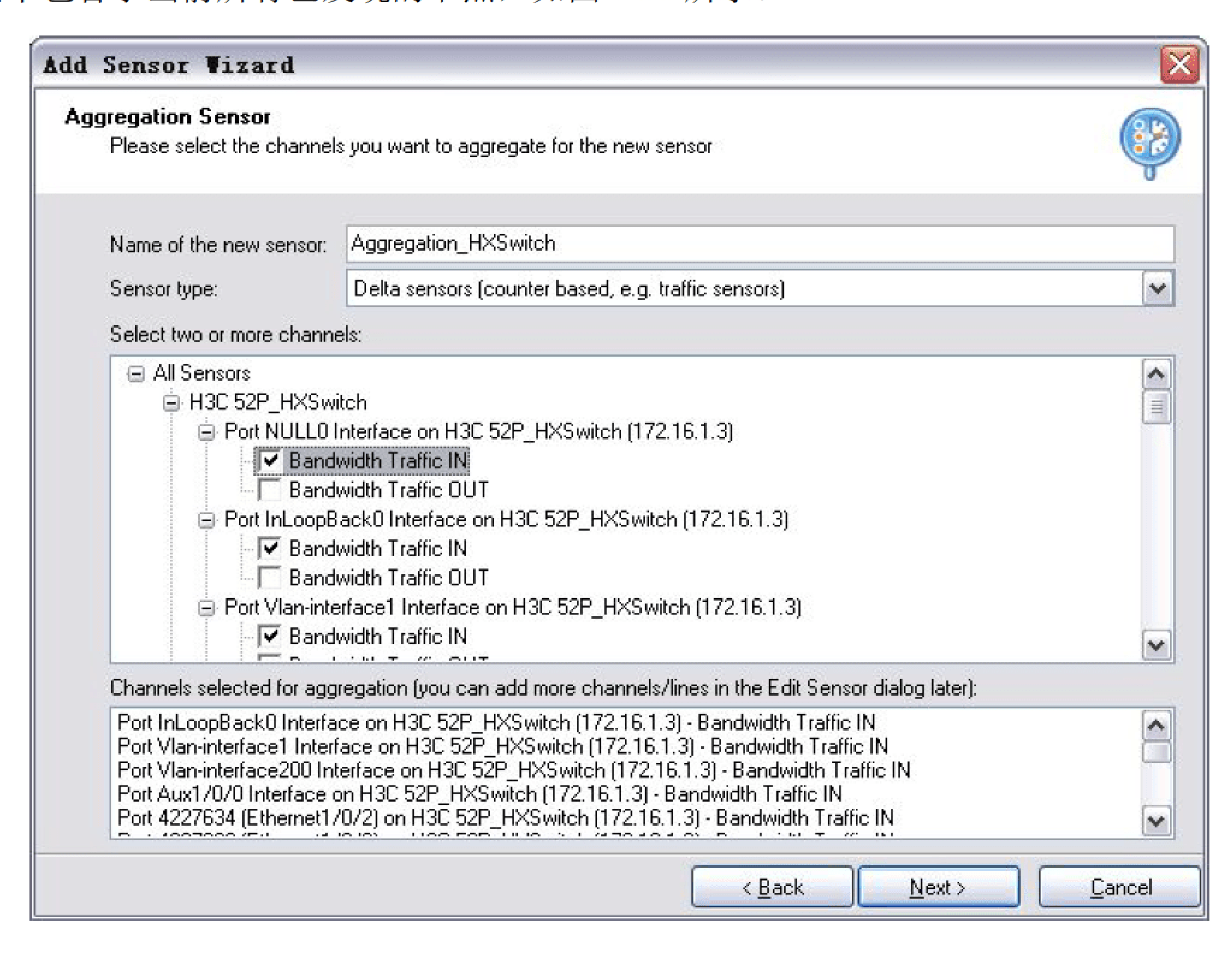


图 9-36　在聚合节点监测方式中选择节点

在节点选择界面将列出可用的节点、接口及其性能监测对象，选择所需网络节点并输入新建聚合节点的名称后即完成设置。查看对应的流量图，将呈现单一的合计值图形，如图 9-37 所示。

注意：该方式下，无法选择不同类别的节点进行聚合（如网卡端口流量和内存使用量）。该方式仅能实现数据流的聚合。

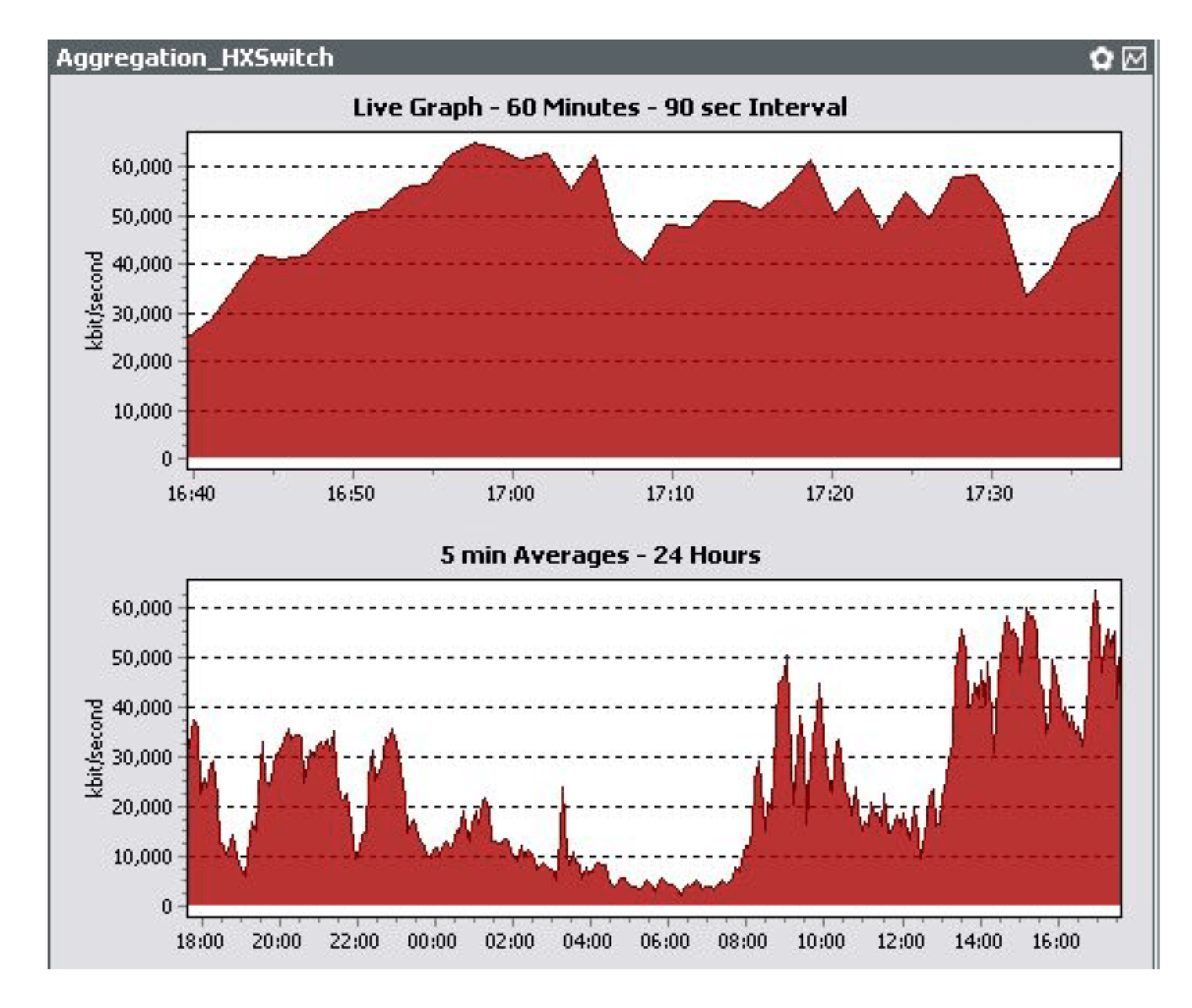


图 9-37 聚合节点的流量图表

9.4.7 3 种带宽监测方式的对比

表 9.1 列出了用于带宽监测的 3 种方式的区别。

表 9.1 3 类 PRTG 带宽监测方式对比

序号	对 比 项 目	SNMP	Packet Sniffing	Netflow
1	配置	简单	复杂程度视过滤条件而定	复杂，需要更改网络设备配置
2	能否通过协议或 IP 地址划分带宽利用率	否	是	是
3	能否展示排名（连接数排名、协议使用情况排名等）	否	是	是
4	通过 IP 地址过滤带宽利用率	否	是	是
5	通过 MAC 地址过滤带宽利用率	否	是	否
6	通过物理端口过滤带宽利用率	是	否	否
7	除带宽利用率之外，能否监测其他参数	是	否	否
8	运行 PRTG 占用的 CPU 负载	低	较高，取决于流量的大小	较高，取决于流量的大小
9	额外占用网络带宽情况	低	无（除非使用了交换机监测端口）	依赖于流量的大小

9.4.8 自动查找和添加网络设备

PRTG 还提供了自动查找和添加网络设备的功能。在主界面中，选择主菜单命令 Extras，该菜单中列出了 PRTG 的附加设置项目，包含自动查找网络节点功能，可按照设定的 IP 地址范围查找并监测网络设备流量。Extras 菜单列表如图 9-38 所示。

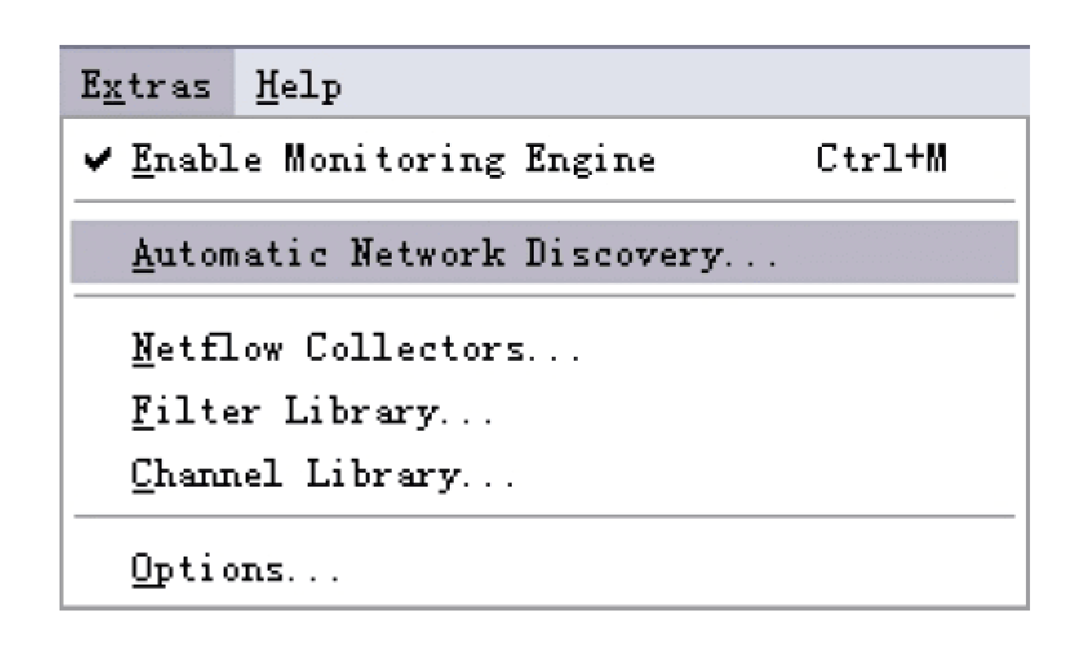


图 9-38 Extras 菜单命令

设置自动查找和添加设备步骤如下：

（1）选择 Extras | Automatic Network Discovery 菜单命令，进入自动发现设置界面，输入 IP 地址的起始段和结束段后，PRTG 将在地址段内逐一搜索每个 IP。如设备 SNMP 社区字符串不是默认的 Public，则更改 SNMP Community String 内容，如未使用默认的 SNMP 端口，则相应更改 SNMP 端口，如图 9-39 所示。

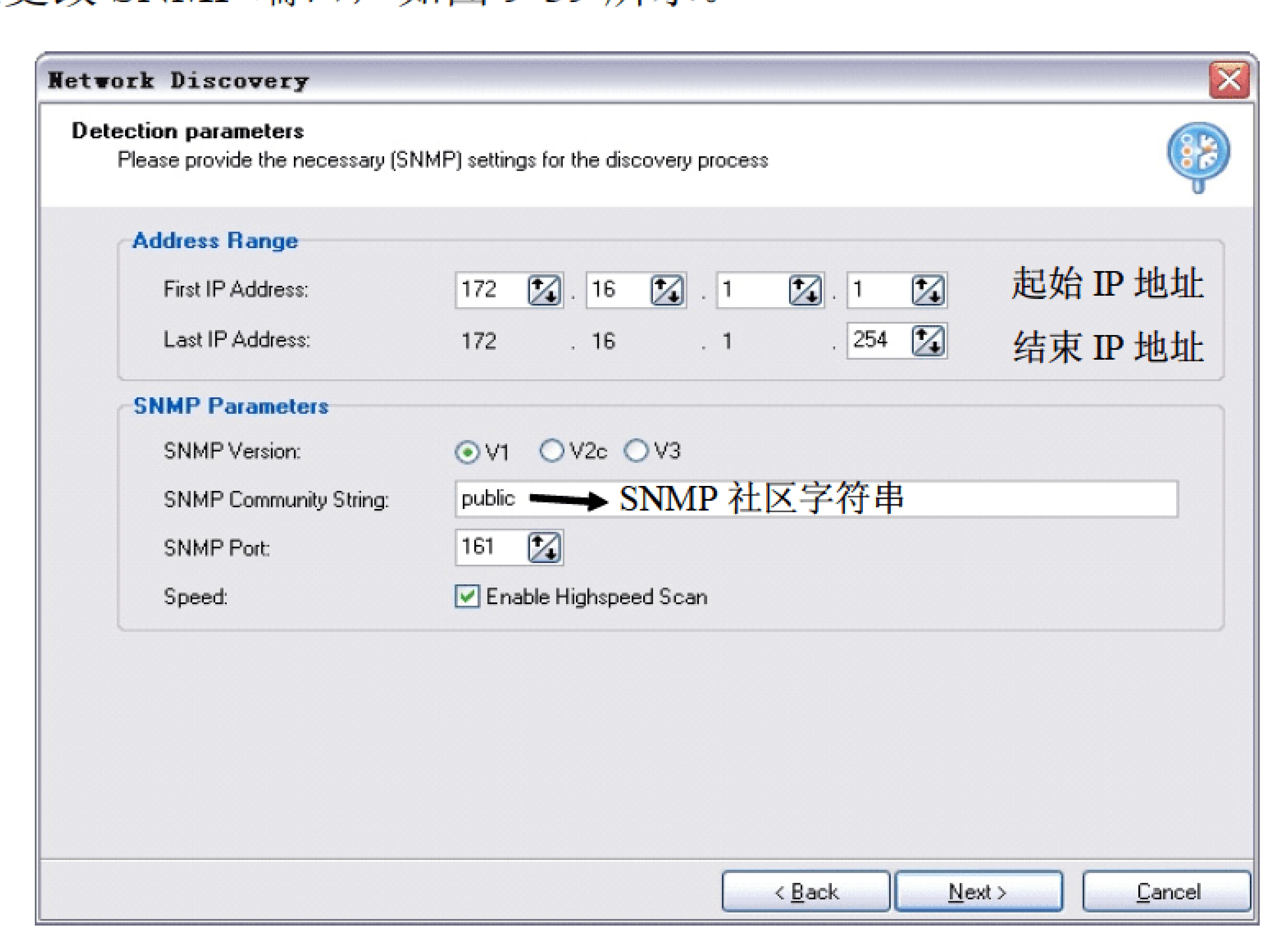


图 9-39 自动发现设备设置窗口

（2）设置完毕后，单击 Next 按钮开始节点的扫描，如图 9-40 所示。

（3）扫描完成后将会列表显示搜索出的网络节点及其端口，选择要监测的设备及其端口即可完成节点的添加，如图 9-41 所示。

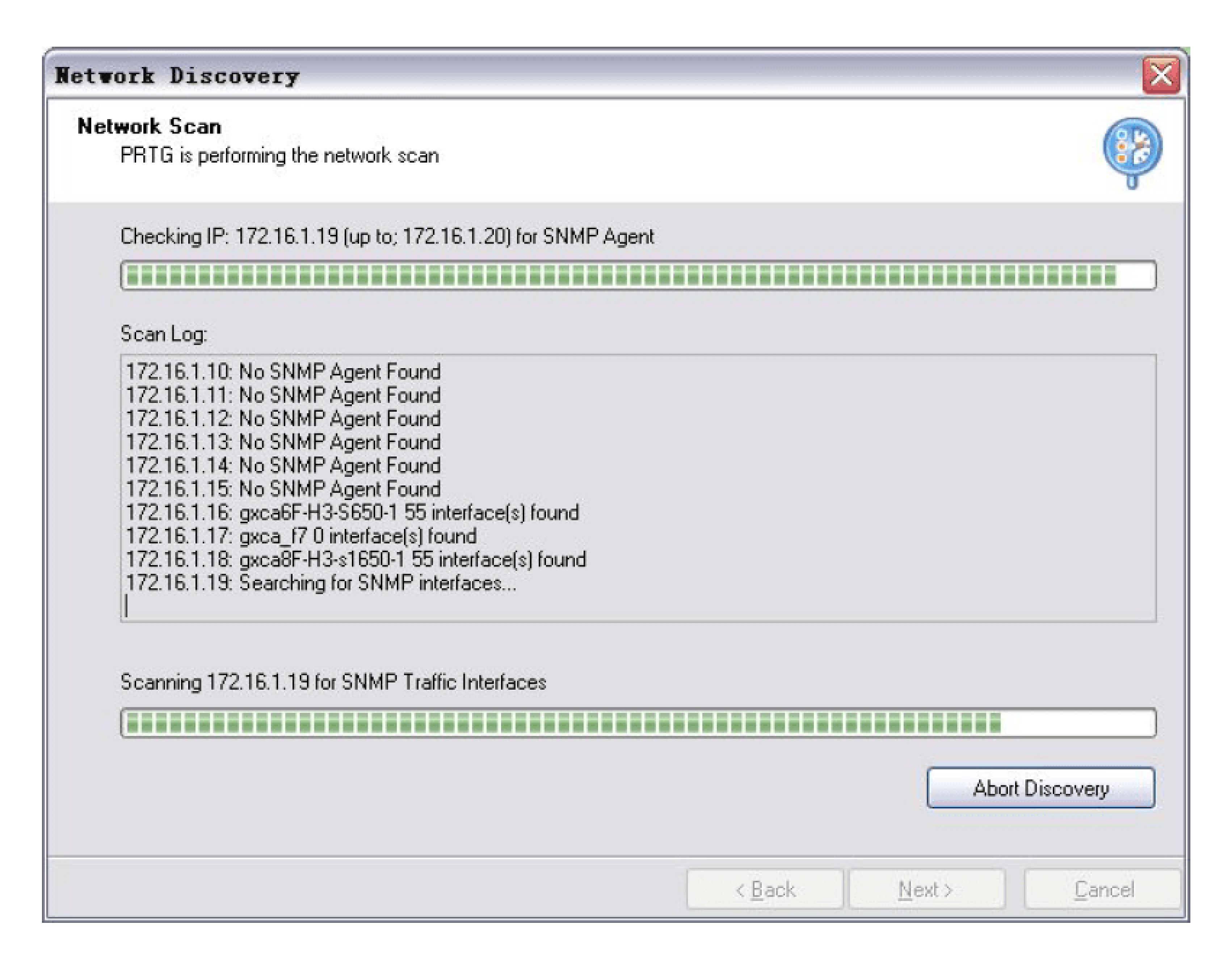


图 9-40　自动扫描发现网络节点

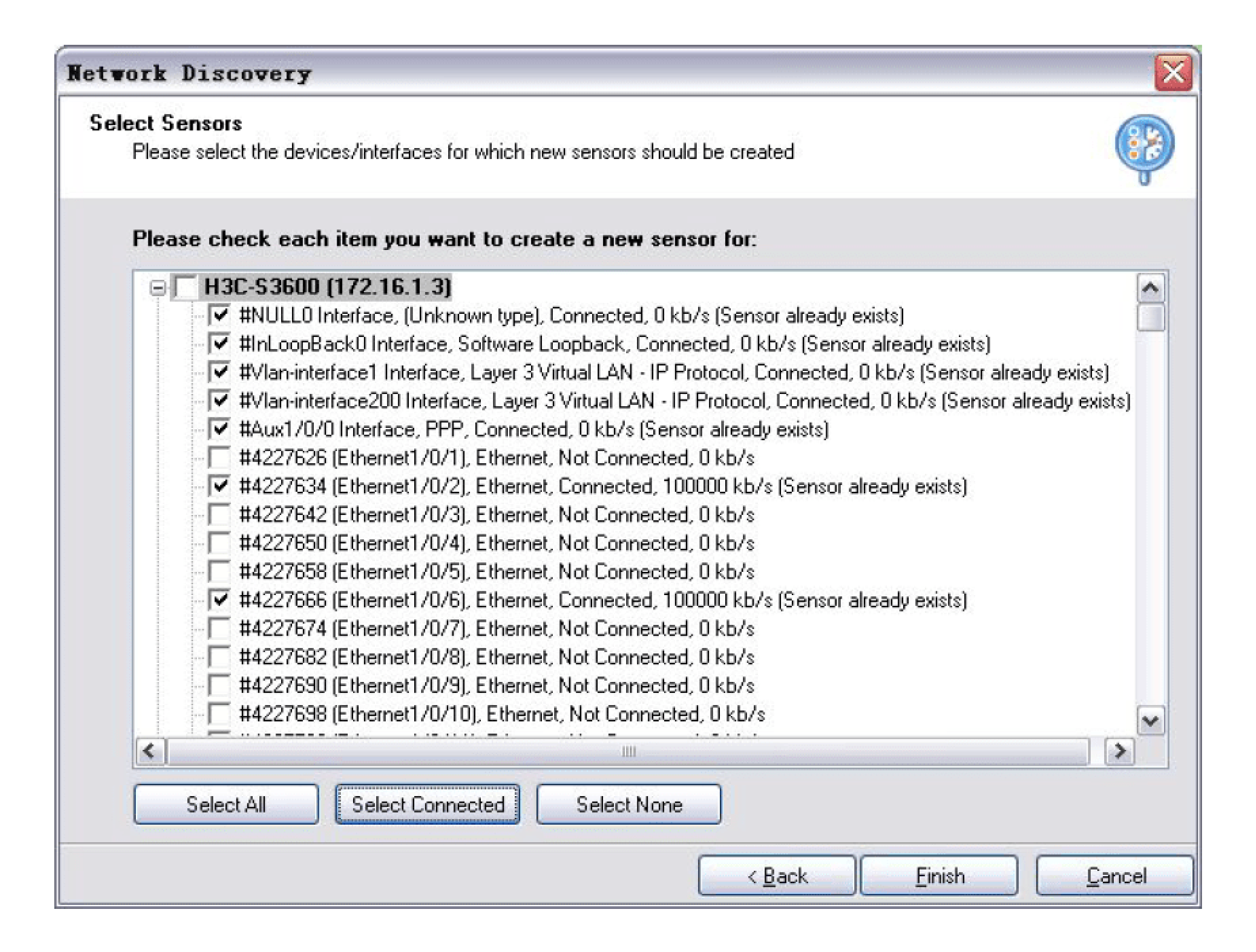


图 9-41　自动扫描方式查找到的设备及接口

注意：未连接的端口或在 PRTG 中已经添加过的设备在扫描完成后不进行添加。

（4）添加节点后，在主界面节点列表中可看出，指定 IP 段内自动发现了 4 个网络设备，如图 9-42 所示。

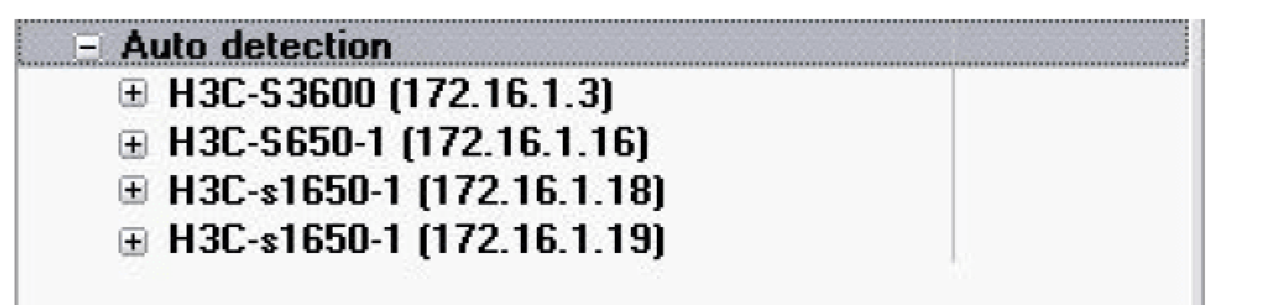


图 9-42　自动扫描发现的设备

（5）选择节点列表中的某设备（如 177.16.1.3），可查看该设备所有选中的端口流量，分别用不同颜色的曲线进行表示，可一目了然看到占用带宽最大的端口，如 9-43 所示。

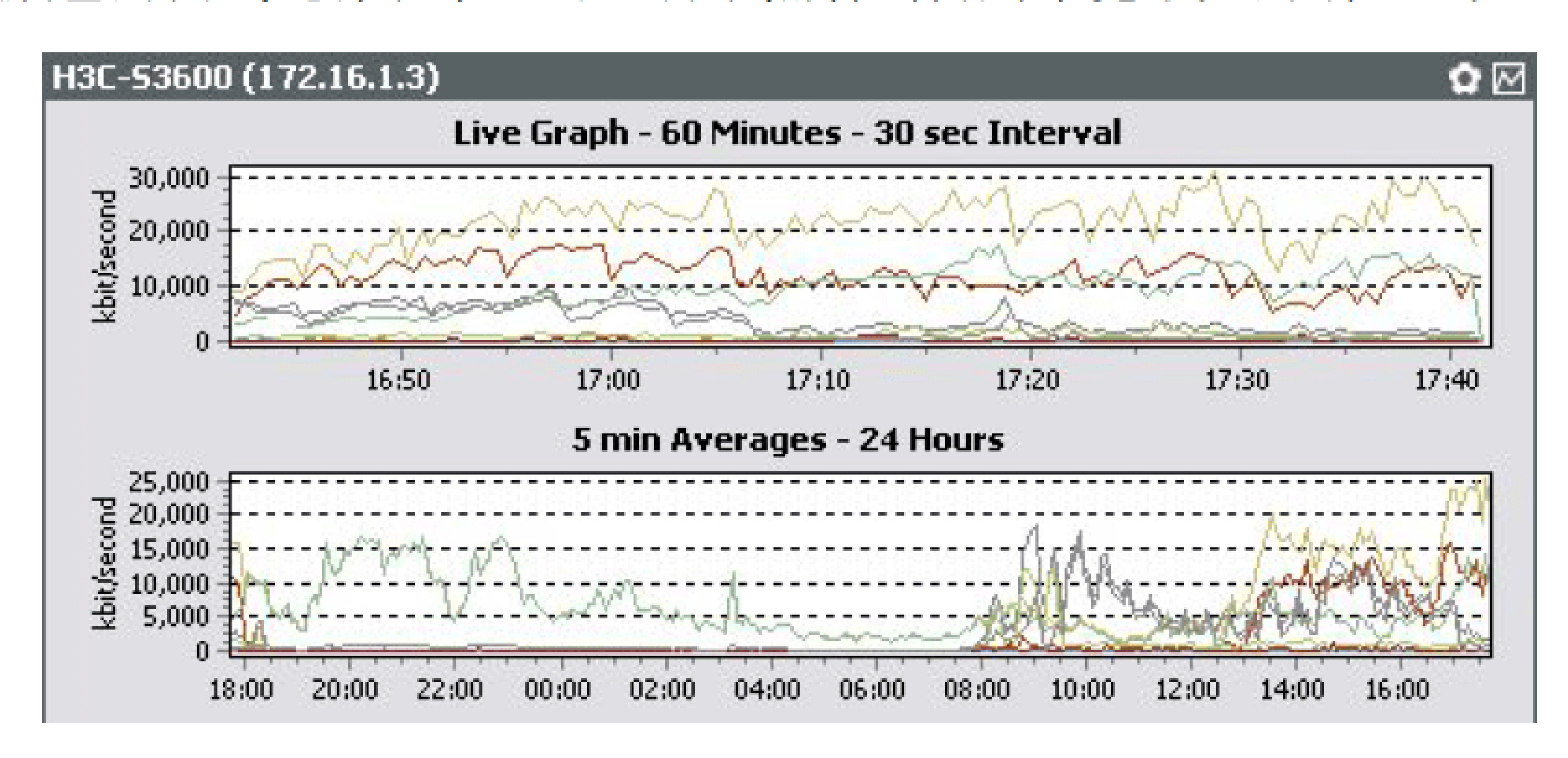


图 9-43　查看交换机设备的各端口流量

9.5　本章小结

本章首先介绍了 PRTG 和辅助程序 SNMP Helper 的概念和安装过程，其安装方式较为简单，不需要做太多设置。然后介绍了使用 PRTG 查找和添加设备的方式，可分为 4 类，分别是通过 SNMP 协议监测网络节点；通过数据包探测方式监测本地网卡数据流；通过 Netflow 方式监测 Cisco 网络设备流量；监测访问设备响应时长，以及监测各节点的聚合数据流。

PRTG 使用者需要明确本地网络结构、设备简单配置及需要监测的对象，选择适合实际情况的监测方式。

第 10 章　PRTG 功能及设置项详解

在查找并添加了网络监测节点后，PRTG 即开始实时地监测网络节点。网管员在此基础上，还需要了解各监测对象的属性和配置，理解监测得到的图表和数据的实际意义，以及在发生异常状态时采取的措施等，达到对 PRTG 的熟练配置和应用。

本章主要介绍主界面各类视图和功能及各功能的详细配置。

10.1　主界面视图介绍

在添加了监测节点后，在主界面中将列出各监测节点及实时展示所选节点的数据流量图表或数据表。在主界面中，主要分为 4 个区域，如图 10-1 所示。

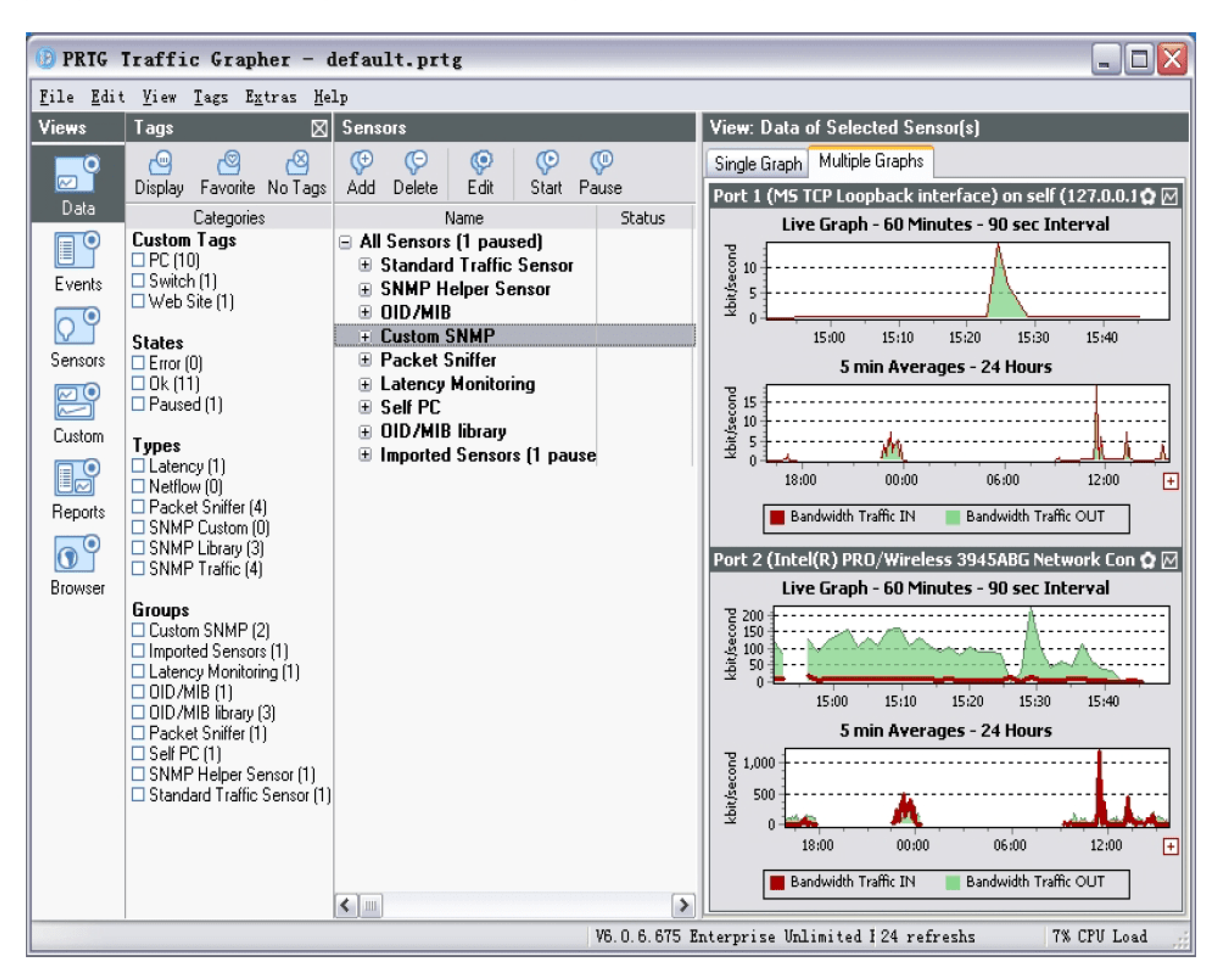


图 10-1　主窗口界面

- ❑ Views：视图区域，共提供了 6 种视图界面；

- Tags：节点分类区域，可按节点标记、状态、类型和类别组显示对应节点信息；
- Sensors：节点列表，可单选或多选节点进行查看，双击可进行节点编辑；
- Data of Selected Sensor：节点图表显示区域，可按照曲线图或数据表展示数据。

以下分别对各区域进行介绍。首先介绍 Views 区域所提供的 6 种视图，如图 10-2 所示。

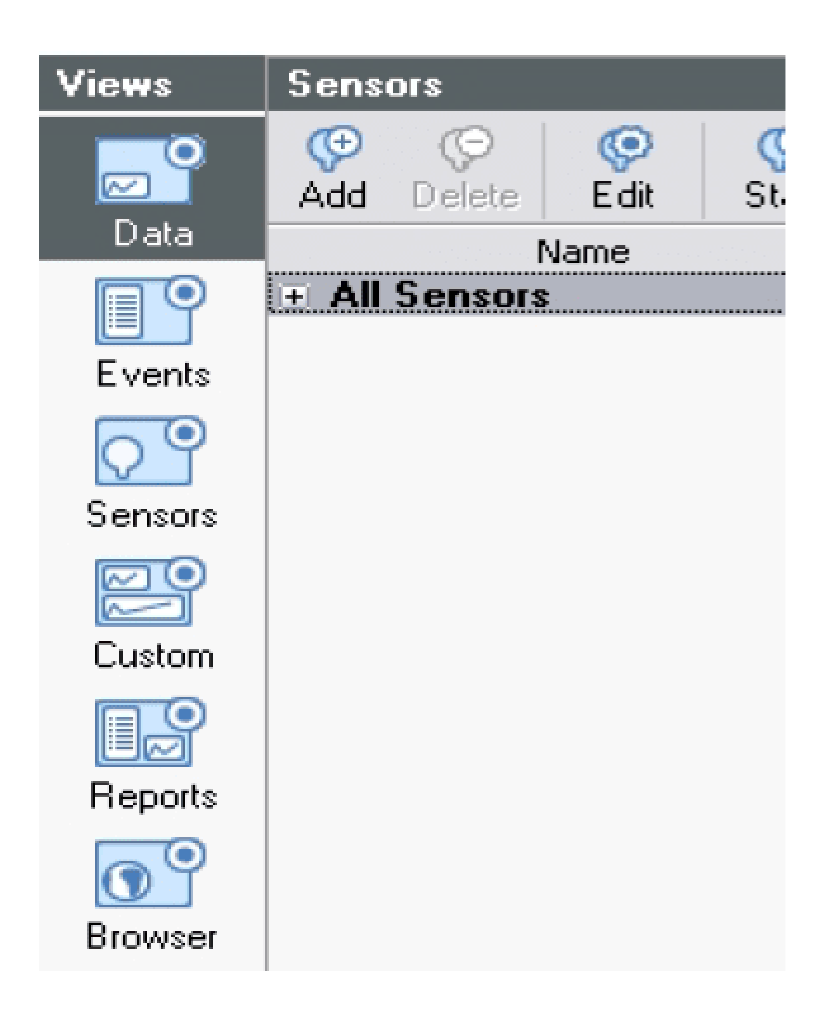


图 10-2　PRTG 中提供的 6 种视图选项

这 6 种视图描述如下。

- Data：在图形界面或表格中，显示一个或多个节点采集到的数据；
- Events：列表显示所有节点或所选的节点发生的事件，如错误提示；
- Sensors：所有节点的管理和组织视图；
- Custom：根据用户需要建立自定义布局的图形、图表和表格；
- Reports：根据用户需求建立的报表；
- Browser：从该处进入 PRTG 的网页接口模式。

下面详解这 6 种视图所能展现的数据。

10.1.1　Data 数据显示视图

1．Data 显示窗口——曲线图表

Data 窗口中，可通过曲线图、表格等多种形式展示。曲线图展示可分为单曲线图和多曲线图。选择单曲线图方式 Single Graph，则在同一个图表中展示多个节点的多条数据曲线；选择多曲线图方式 Multiple Graph，可在多个图表中分别展示各节点数据曲线，如图 10-3 所示。

选择某一个监测节点，在主界面中默认显示该节点的曲线图 Graph，并提供了该单一节点 4 个层次的数据显示图表，可通过双击某图表进行放大显示，4 个层次图表分别介绍如下。

- Live Graph – 60 Minutes – 30 Sec Interval：实时流量曲线图，每间隔 30 秒做一次流

量采集，界面中共展现了 60 分钟长度的实时流量状态，采集信息的时长可自行设置。

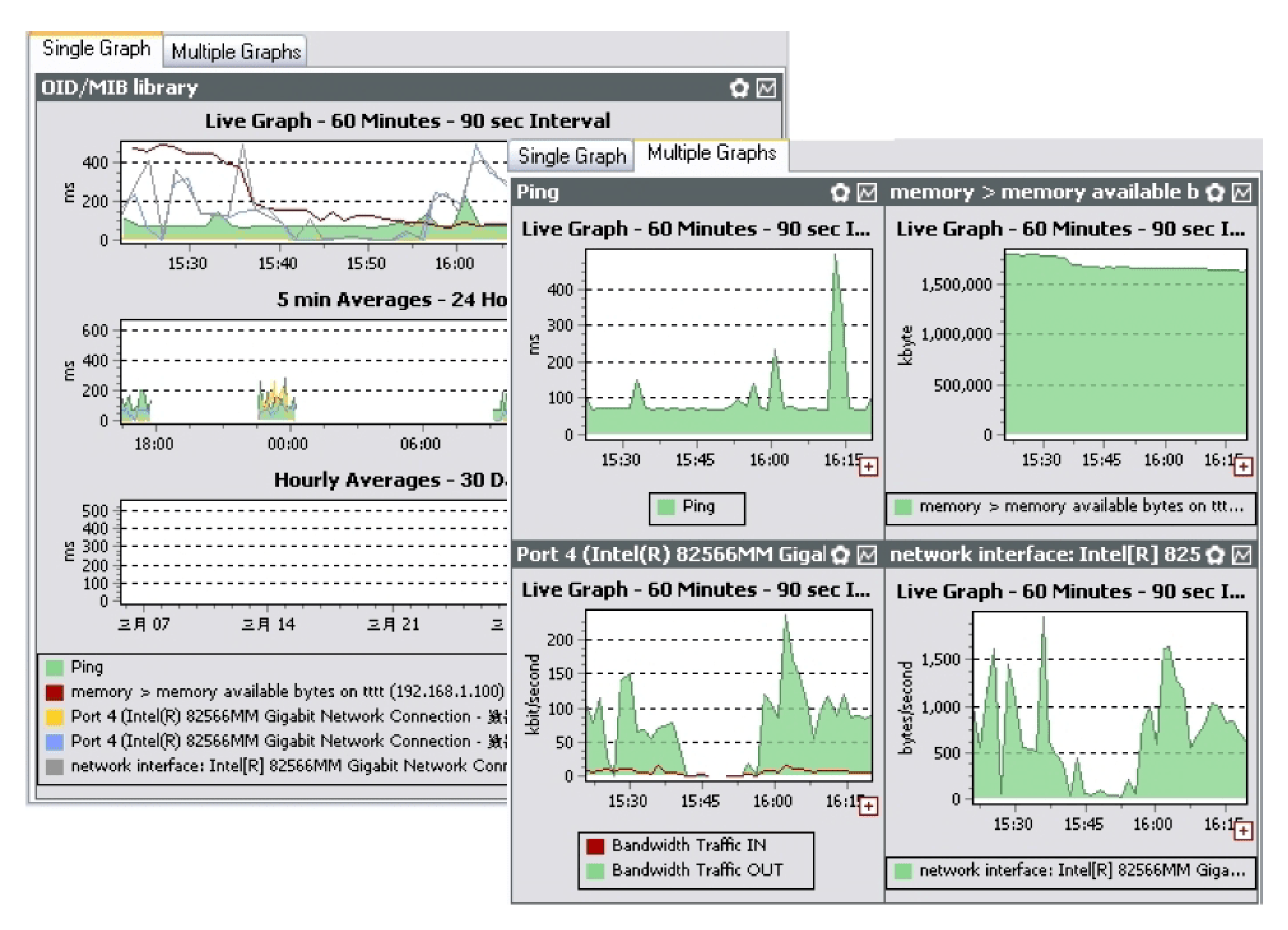


图 10-3　数据图形显示方式

- ❑ 5 Min Averages – 24 Hours：显示前 5 分钟的流量平均值，界面中共展现 24 小时长度的流量状态。
- ❑ Hourly Averages – 30 Days：显示前 1 小时的流量平均值，界面中共能展现 30 天长度的流量状态。
- ❑ Daily Averages – 365 Days：显示前 1 天的流量平均值，界面中共能展现 365 天长度的流量状态。

如果需要更改图像中记录信息的时间周期，可选择主界面的菜单命令 Extras | Options | User Interface，在属性设置界面中进行更改，如图 10-4 所示。

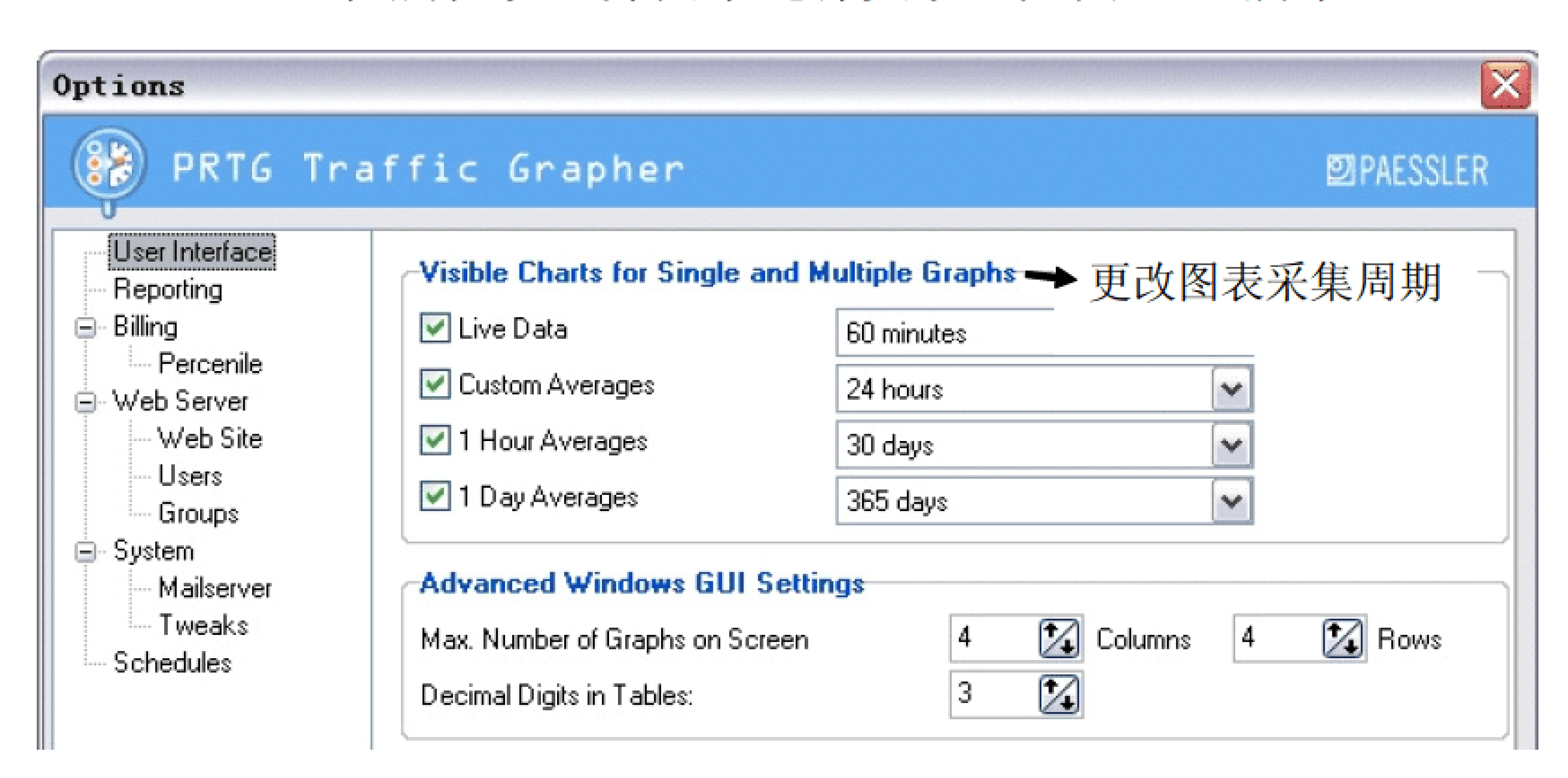


图 10-4　配置图像记录信息的时间周期

2. Data 显示窗口——数据表格

在表格显示中，提供前 24 小时、前 30 天和前 365 天的监测数据，数据流类的节点主要包含容量和速率平均值两部分。默认 24 小时数据表是由每 5 分钟内接收到的数据量和 5 分钟内的流量速率平均值组成；30 天数据表由每小时的数据量和每小时内的速率平均值组成；365 天数据表由每一天内的数据量和一天内的速率平均值组成。

该显示周期与曲线图相对应，也能根据需要进行调整。数据表种类如图 10-5 所示。



图 10-5　Data View 中的表格数据种类

注意：数据流类型类节点有 Top 类数据，而计算机性能类节点（如磁盘利用率）则没有。

由于 PRTG 监测节点的种类不同，所以在曲线图和数据表格中展现的内容也有所不同。下面分别介绍不同类型节点的数据展现形式。

（1）如果选择节点为 SNMP 监测，或者包探测模式未选择协议监测时，在数据表格中将按照小时作为时段显示统计信息，包括数据流出、流入的流量统计及合计信息等，如图 10-6 所示。

Graph | Table: 24 Hours | Table: 30 Days | Table: 365 Days

Table: Port 4228002 (Ethernet1/0/48) on H3C 52P_HXSwitch (172.16.1.3) (30 Days, Hourly Averages)

	Port 4228002 (Ethernet1/0/48) on H3C 52P_HXSwitch (172.16.1.3)						
	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum		Coverage
	megabyte	megabyte/second	megabyte	megabyte/second	megabyte	megabyte/second	%
2010-4-6 14:00 - 15:00	1,124.086	0.320	5,135.424	1.463	6,259.510	1.783	98
2010-4-6 13:00 - 14:00	1,401.534	0.396	5,791.774	1.636	7,193.308	2.032	98
2010-4-6 12:00 - 13:00	1,316.414	0.381	4,444.020	1.288	5,760.434	1.669	96
2010-4-6 11:00 - 12:00	825.045	0.233	1,927.568	0.545	2,752.613	0.778	98
2010-4-6 10:00 - 11:00	2,508.300	0.715	338.345	0.096	2,846.645	0.811	97
2010-4-6 9:00 - 10:00	1,898.300	0.537	281.401	0.079	2,179.701	0.616	98
2010-4-6 8:00 - 9:00	789.228	0.233	202.117	0.060	991.345	0.293	94
2010-4-6 7:00 - 8:00	31.738	0.009	11.940	0.004	43.678	0.013	94

图 10-6　Data View 中的表格按数据合计显示

注意：Coverage 字段表示在对应的时间周期内，监测实际运行时间所占周期的比率。如果在每小时的监测周期内，PRTG 运行了 45 分钟，则该值显示为 75%。如果需要可靠完整的数据，则应保持该值为 100%或接近 100%。如果 PRTG 一直为运行状态，但采集数据仍不完整，有可能存在网络问题，例如连接失败、丢包的情况。

（2）如果选择节点为包探测模式，选择了协议对象进行监测，则在表格中将按照所选协议进行分类统计，以及显示合计信息，如图 10-7 所示。

（3）如果选择节点为 Packet Sniffer 包探测节点或 NetFlow 数据流节点，则在 Data 数据表格中增加了 3 项 Top 数据显示种类。Top 数据列表主要按照目的 IP 地址和端口进行排序，包括 Top Talkers（最活跃的目的 IP 地址排行）、Top Connections（两个设备间连接最

活跃的排行）、Top Protocols（按最活跃的协议排行）。

Graph | Table: 24 Hours | Table: 30 Days | Table: 365 Days | Top Talkers | Top Connections | Top Prot

Table: Packet Sniffing_pc (30 Days, Hourly Averages)

	Packet Sniffing_pc					
	Other		DNS		FTP	
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second
2010-4-6 15:00 - 16:00	6,235,188.677	14,189.267	16.996	0.039	0.000	0.000
2010-4-6 14:00 - 15:00	5,392,479.718	12,271.535	13.068	0.030	0.000	0.000
2010-4-6 13:00 - 14:00	6,076,443.528	13,827.976	15.187	0.035	0.000	0.000
2010-4-6 12:00 - 13:00	4,812,547.621	10,951.797	16.355	0.037	0.000	0.000
2010-4-6 11:00 - 12:00	1,898,869.777	4,321.212	163.845	0.373	3.371	0.008
2010-4-6 10:00 - 11:00	1,928.037	4.388	28.634	0.065	0.000	0.000

图 10-7　Data View 中的表格按协议分类显示

Top 数据也能够根据需要进行配置，默认在 Top 数据列表中均以兆每秒（megabytes/second）为单位，如图 10-8 所示。

Graph | Table: 24 Hours | Table: 30 Days | Table: 365 Days | Top Talkers | Top Connections | Top Protocols

Top Talkers: Packet Sniffing_pc

2010-4-6 17:00:00 - 2010-4-6 17:15:00 (Note: Doubleclick the list to access previous intervals

	IP	Volume	Trend (34%)
2	[172.16.1.3]	209 kbytes	+53
3	[172.16.1.16]	109 kbytes	+58
4	[172.16.1.18]	109 kbytes	+58
5	SHENSHENG1 (172.16.6.22)	96 kbytes	>96
6	[172.16.1.19]	66 kbytes	+59
7	Broadcast (255.255.255.255)	66 kbytes	+59
8	DOMAIN (172.16.1.1)	57 kbytes	+67
9	PC-200905201121 (172.16.6.91)	31902 bytes	-7

图 10-8　Data View 中的表格按 Top 数据显示

注意：Trend 字段表示实体在当前列表中的位置，通过减去它在上一周期列表中的位置计算机而出。如果数值为 0，表示该实体在当前列表位置与上一周期列表位置相同；+5 表示该实体上升了 5 个位置；如果数值较大，表示该实体数值变化较为异常，在 PRTG 表格中，将用红色作为背景色进行提醒。

在 Top 列表中，同样显示了按照 IP 地址和端口排名的饼图和柱状图，如图 10-9 所示。

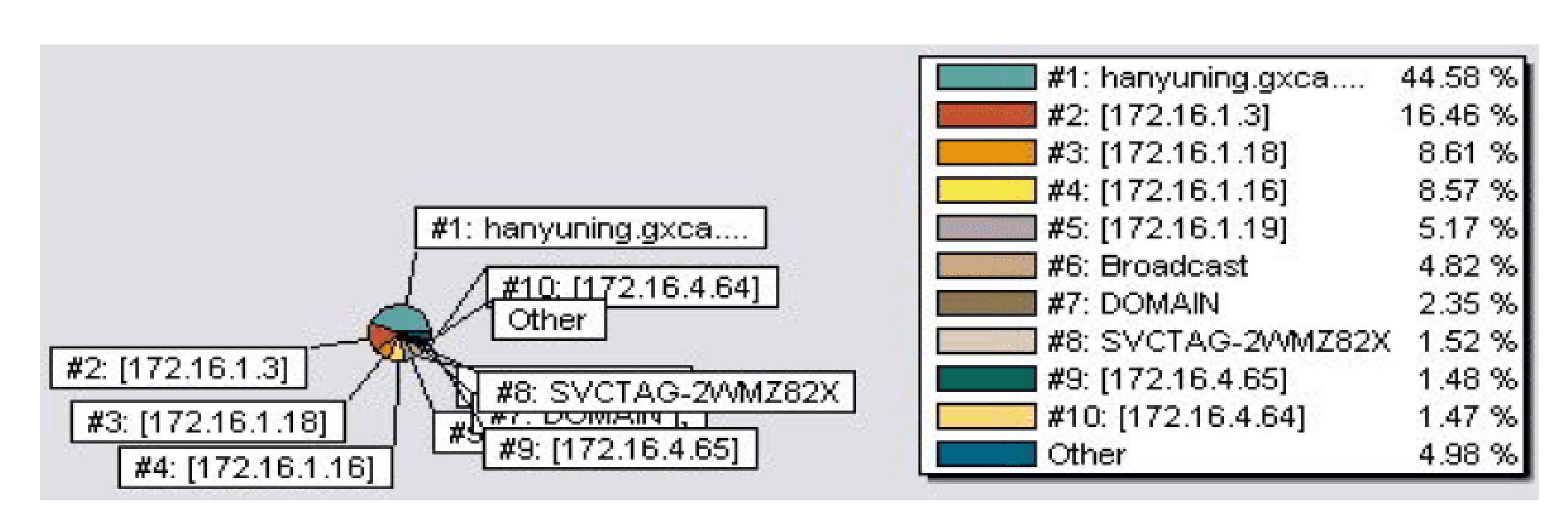


图 10-9　按照 IP 地址和端口排名的饼图和柱状图

（4）如果在数据视图中，显示区域较小使得查看数据不便，那么可在某数据表中双击表格或选择右键菜单中的 View Details 命令（如图 10-10 所示），将在展开的明细界面中显示数据表。

Graph | Table: 24 Hours | Table: 30 Days | Table: 365 Days | Top

Table: PC-200909132216 (24 Hours, 5 min Averages)

	PC-200909132216			
	Other		DNS	
	kbyte	kbit/second	kbyte	kbit/
2010-4-4 17:25 - 17:30				
2010-4-4 17:20 - 17:25				
2010-4-4 17:15 - 17:20	4,256.114	6.117	0.000	
2010-4-4 17:10 - 17:15	5,816.181	158.831	0.000	

View Details...
Change Colors & Layout...

图 10-10　展开某数据表

在明细表界面中，可将数据保存为 HTML 格式或 Excel 格式。在表格中打开右键菜单，选择 Save Table to XLS...命令，即可导出并保存为 Excel 文件，如图 10-11 所示。

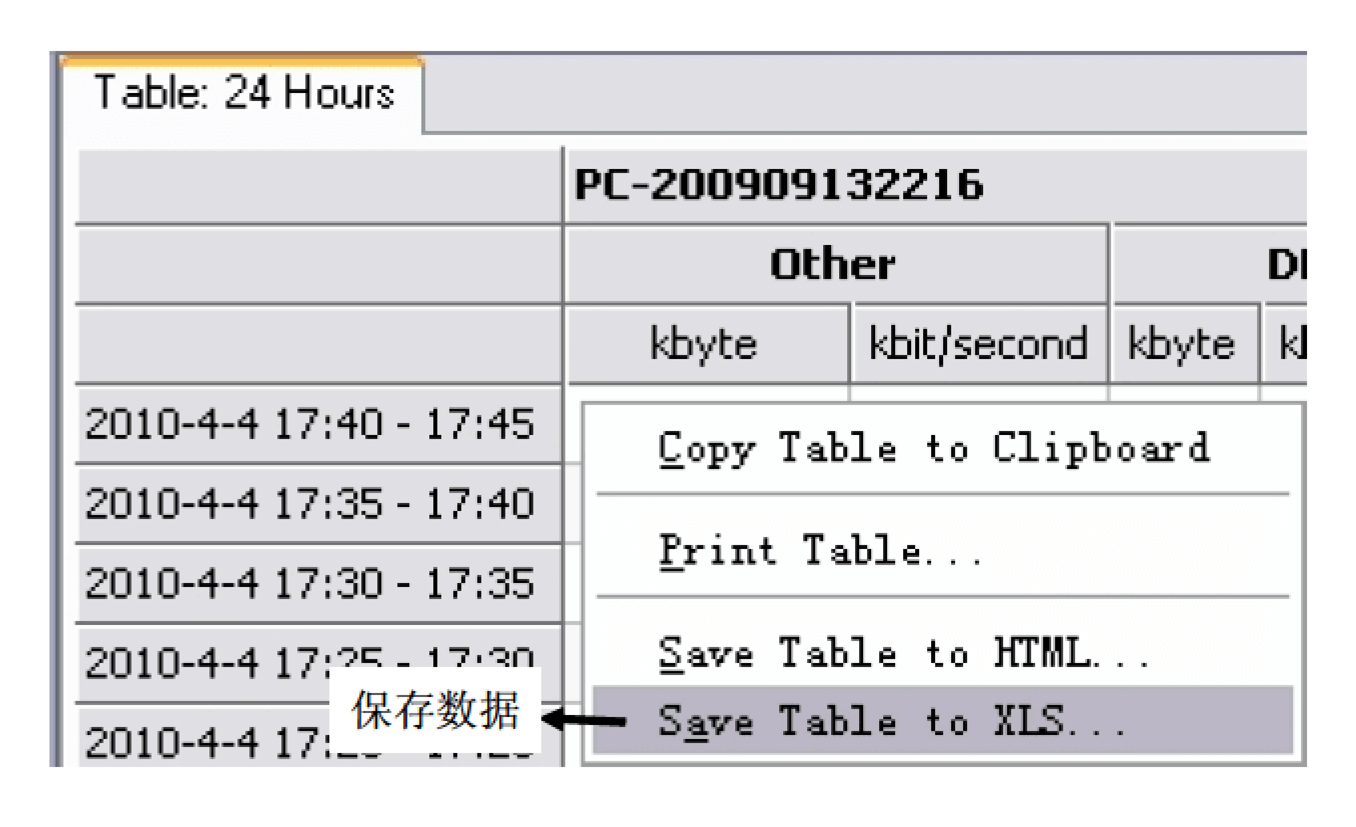


图 10-11　手动导出 Table 数据

10.1.2　Events 事件列表视图

每当节点出现异常，或重新恢复正常状态，或提示信息被触发，PRTG 将对这些信息进行记录，在 Events 列表中能够查看事件信息，如图 10-12 所示。

10.1.3　Sensors 节点信息视图

在节点视图中，列出了所有添加的监测节点，并列出了各个节点名称和 IP 地址、当前的状态、最小采集时间周期、节点类型及备注信息。当设备出现故障（或无法连接、网络

故障等）将通过红色背景色做出标识，如图 10-13 所示。

View: Events

Time	Kind	Sensor
2010-4-4 9:13:31	Error	Ping
2010-4-4 9:01:48	Error	Ping
2010-4-4 9:01:03	Error	Port 4 (Intel(R) 82566MM Gigabit Network Connection - 数据包计划程序微型端
2010-4-3 22:38:09	Error	Ping
2010-4-3 22:36:41	Error	Ping
2010-4-3 22:36:13	Error	Port 4 (Intel(R) 82566MM Gigabit Network Connection - 数据包计划程序微型端
2010-4-3 22:34:43	Error	Port 4 (Intel(R) 82566MM Gigabit Network Connection - 数据包计划程序微型端
2010-4-3 11:23:53	Error	Port 4 (Intel(R) 82566MM Gigabit Network Connection - 数据包计划程序微型端
2010-4-3 11:22:44	Error	Port 3 (Intel(R) 82566MM Gigabit Network Connection - 数据包计划程序微型端
2010-4-3 11:22:23	Error	Port 4 (Intel(R) 82566MM Gigabit Network Connection - 数据包计划程序微型端

图 10-12　Views 事件记录

Sensors

Add　Delete　Edit　Start　Pause

Name	Status	Device
All Sensors (20 errors)		
H3C 52P_HXSwitch (5 errors)		
Port NULL0 Interface on H3C 52P_HXSwitch (172.16.1.3)	0 kbit/second	H3C 52F
Port InLoopBack0 Interface on H3C 52P_HXSwitch (172.1	Error	H3C 52F
Port Vlan-interface1 Interface on H3C 52P_HXSwitch (172	0 kbit/second	H3C 52F
Port Vlan-interface200 Interface on H3C 52P_HXSwitch (1	0 kbit/second	H3C 52F
Port Aux1/0/0 Interface on H3C 52P_HXSwitch (172.16.1	0 kbit/second	H3C 52F
Port 4227634 (Ethernet1/0/2) on H3C 52P_HXSwitch (17	3 kbit/second	H3C 52F
Port 4227666 (Ethernet1/0/6) on H3C 52P_HXSwitch (17	3 kbit/second	H3C 52F
Port 4227890 (Ethernet1/0/34) on H3C 52P_HXSwitch (1	34 kbit/second	H3C 52F
Port 4227906 (Ethernet1/0/36) on H3C 52P_HXSwitch (1	Error	H3C 52F
Port 4227922 (Ethernet1/0/38) on H3C 52P_HXSwitch (1	31 kbit/second	H3C 52F
Port 4228002 (Ethernet1/0/48) on H3C 52P_HXSwitch (1	megabyte/second	H3C 52F
Port 4228041 (GigabitEthernet1/1/1) on H3C 52P_HXSwi	2,255 kbit/second	H3C 52F
Port 4228049 (GigabitEthernet1/1/2) on H3C 52P_HXSwi	18 kbit/second	H3C 52F
Port 4228065 (GigabitEthernet1/1/4) on H3C 52P_HXSwi	72 kbit/second	H3C 52F
Port 4228057 (GigabitEthernet1/1/3) on H3C 52P_HXSwi	Error	H3C 52F

图 10-13　节点信息视图

在界面上方导航图标栏中，单击 Add 按钮，即可显示节点添加向导；单击 Delete 按钮可对节点进行删除；单击 Start 按钮和 Pause 按钮可控制节点开始和暂停监测。

注意：在节点列表中，可以通过拖放操作将节点重新划分组。

单击 Edit 按钮可打开节点配置窗口，可对节点属性进行设置，如图 10-14 所示，在该界面中的 Identification 选项中，显示了节点的基本信息（名称、类型等）。

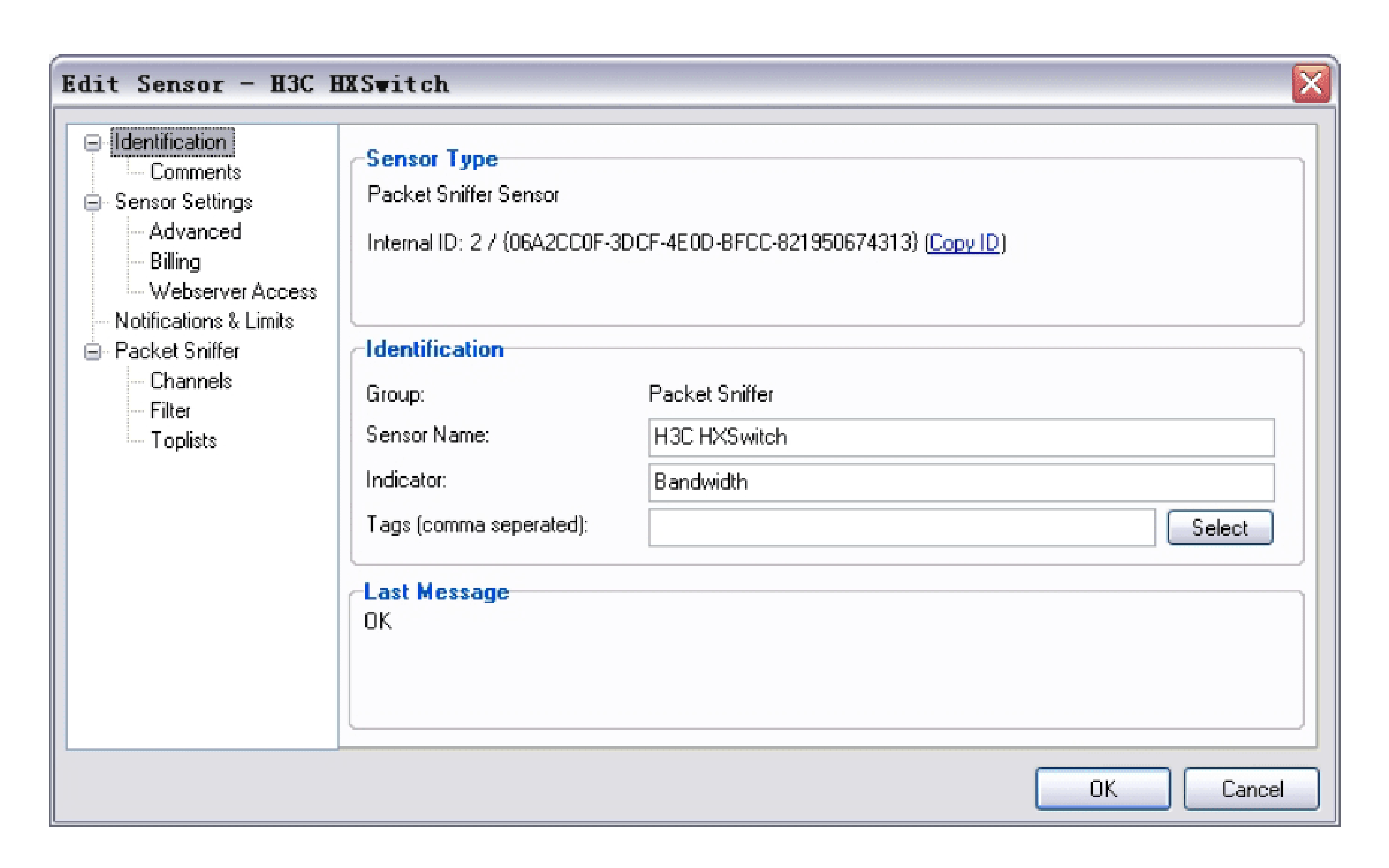


图 10-14　节点配置界面

10.1.4　节点配置——基础属性

以下将对 Edit Sensor 界面中的基础配置项做详细说明，后续部分介绍更多的节点配置。

（1）Comments：备注信息设置，在节点配置界面中选择 Comments，该界面可为该节点增加任何备注信息，备注信息使用简单的 HTML 语法，例如<b>标识为粗体显示，
标识为添加新行等。输入备注之后，将在右侧看到预览的效果。选中 Show Comments on Webpages 复选框，则允许该内容在网页模式中显示，如图 10-15 所示。

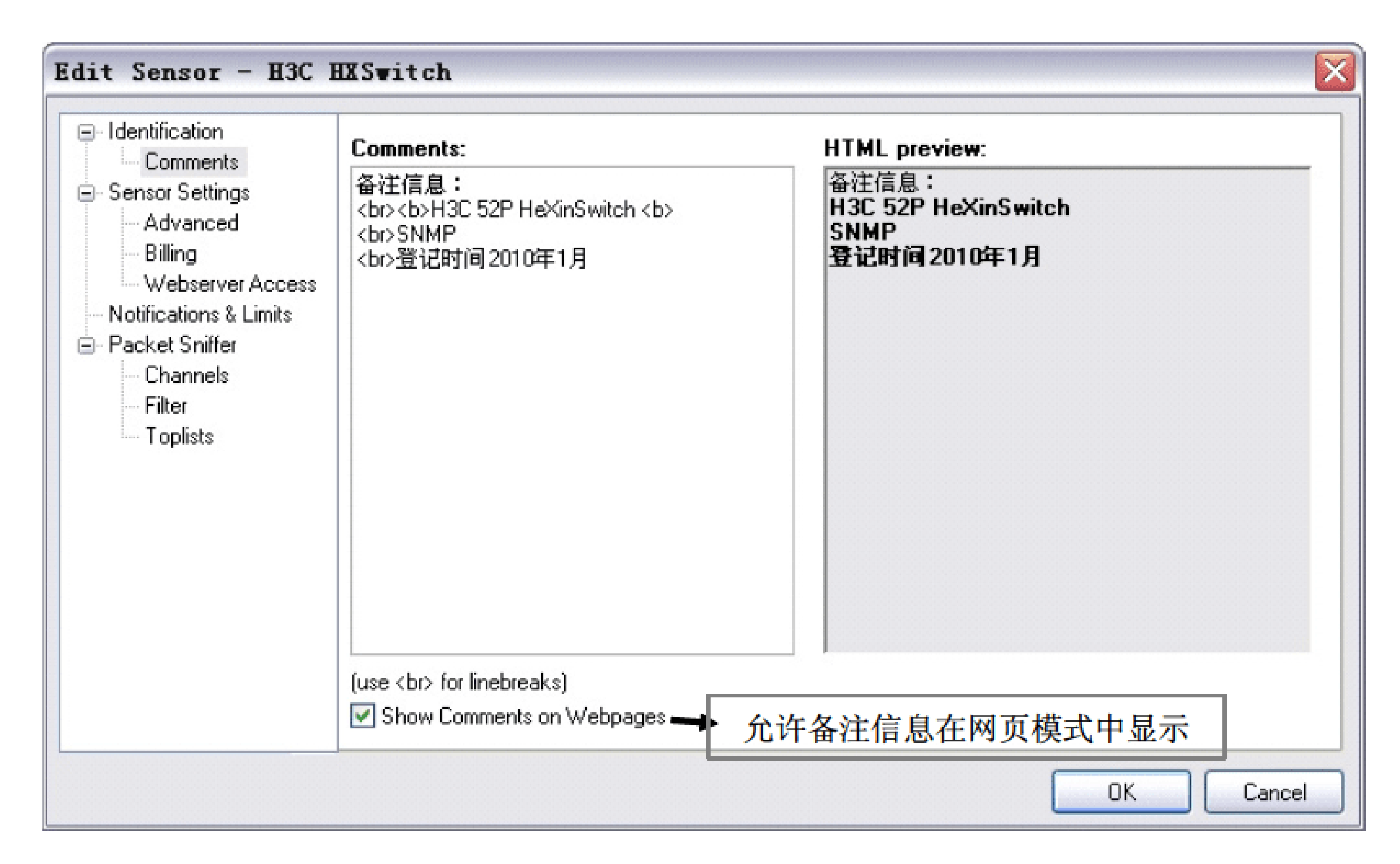


图 10-15　节点配置——添加备注信息

（2）Sensor Settings：节点设置界面，可更改采集数据周期、计算流量平均值时间周期，设置将数据信息保存至 CSV 文档等配置，如图 10-16 所示。

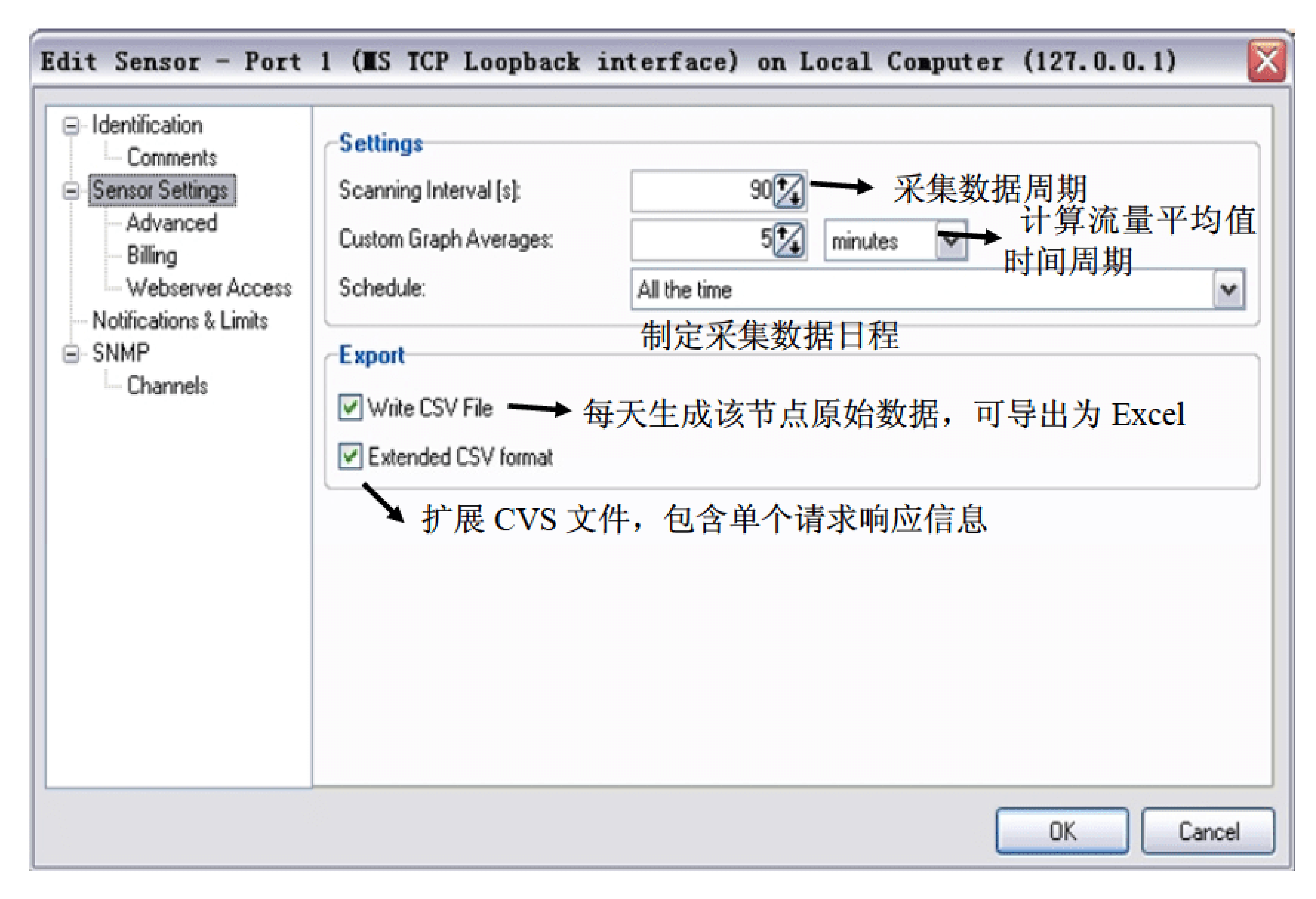
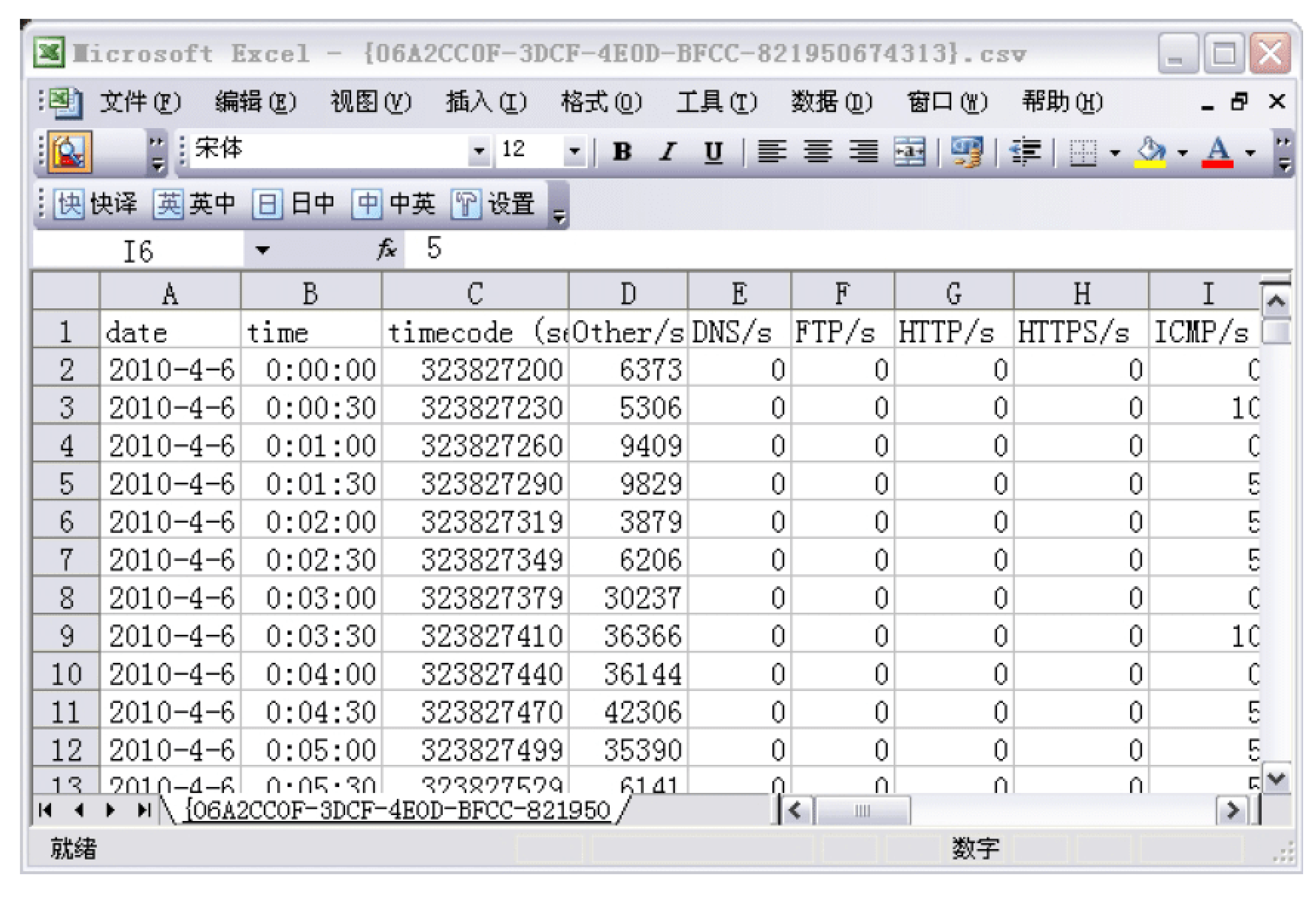


图 10-16　节点配置——配置采集周期和导出信息等

选中 Write CSV Files 复选框，则允许 PRTG 每天为所选节点生成原始监测数据的 Excel 文件，并可导出；选中 Extended CSV format，则允许生成的 Excel 文件中包含更多的数据，能够包含节点每次询问得到的应答信息，并可供导入到其他外部程序中做进一步的分析。

注意：PRTG 每天在 c:\documents and settings\all users\prtg traffic grapher 目录下生成一个用日期命名的文件夹（如 20100321），用于存放当日原始数据信息和生成的 Excel 文件。

打开 Excel 数据文件，即可看到 PRTG 为指定节点保存的统计数据，如图 10-17 所示。



	A	B	C	D	E	F	G	H	I
1	date	time	timecode (s	Other/s	DNS/s	FTP/s	HTTP/s	HTTPS/s	ICMP/s
2	2010-4-6	0:00:00	323827200	6373	0	0	0	0	C
3	2010-4-6	0:00:30	323827230	5306	0	0	0	0	1C
4	2010-4-6	0:01:00	323827260	9409	0	0	0	0	C
5	2010-4-6	0:01:30	323827290	9829	0	0	0	0	5
6	2010-4-6	0:02:00	323827319	3879	0	0	0	0	5
7	2010-4-6	0:02:30	323827349	6206	0	0	0	0	5
8	2010-4-6	0:03:00	323827379	30237	0	0	0	0	C
9	2010-4-6	0:03:30	323827410	36366	0	0	0	0	1C
10	2010-4-6	0:04:00	323827440	36144	0	0	0	0	C
11	2010-4-6	0:04:30	323827470	42306	0	0	0	0	5
12	2010-4-6	0:05:00	323827499	35390	0	0	0	0	5
13	2010-4-6	0:05:30	323827529	6141	0	0	0	0	5

图 10-17　CVS 文件中保存的数据信息

（3）Advanced：高级选项配置，可对数据单位等信息做配置。配置 Volume 属性，可更改原始数据的容量计算单位，默认为 kbyte，即统计单位为字节，可更改为兆字节等。更改 Speed 可配置流量速率单位，默认为 kbyte/s，即为每秒通过的字节数，可更改为每分钟、每小时通过的字节数、兆字节数等，如图 10-18 所示。

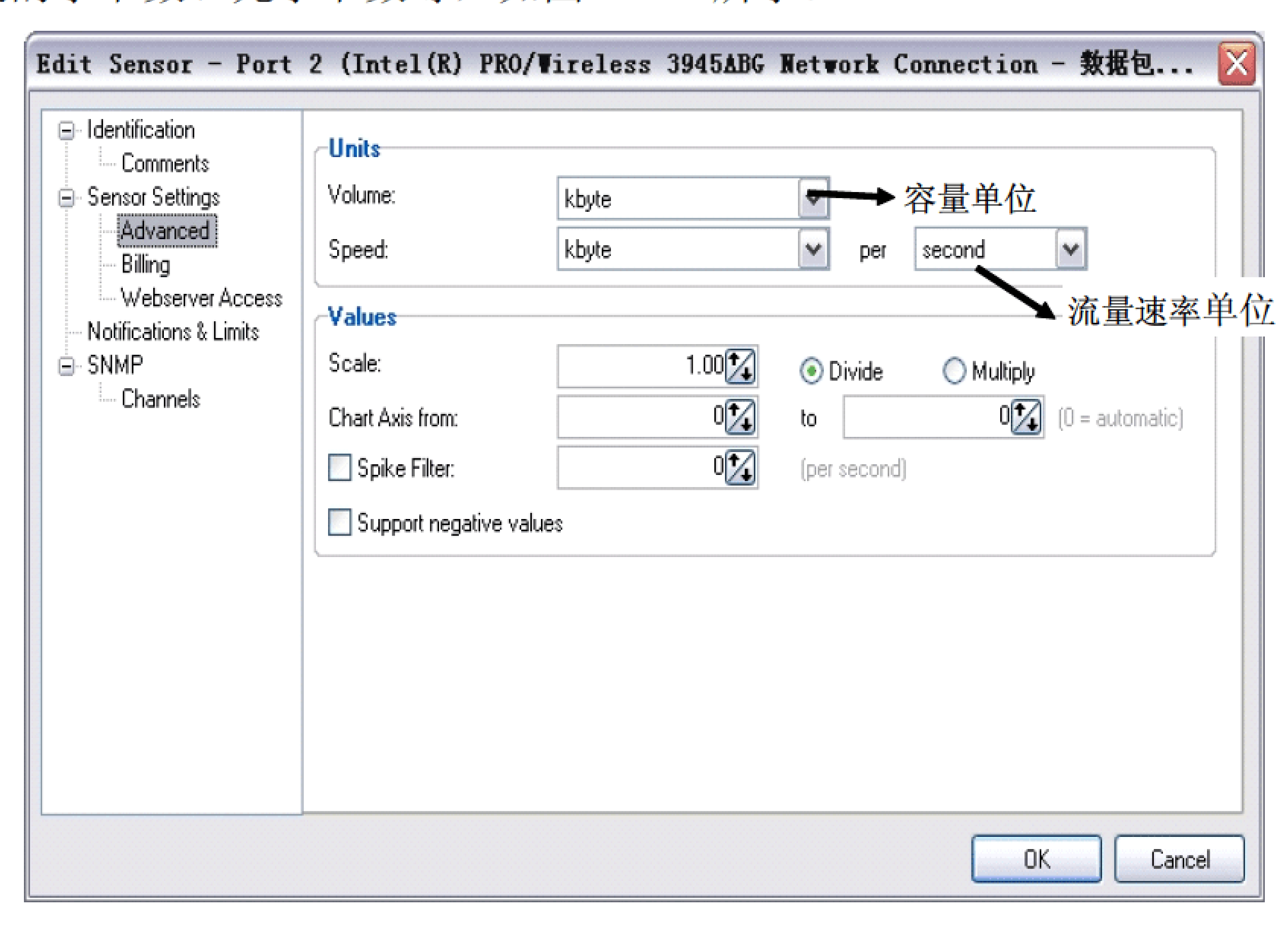


图 10-18　节点配置界面——高级选项

在 Value | Scale 项中还可以更改数据显示的比例。Divide 选项为数据除于所选数值后显示；选择 Multiply 单选按钮则数据乘以所选数值后显示；更改 Chart Axis from …to 参数，可自定义流量曲线图的纵坐标区间值，默认数值为 0，流量曲线图能够按照流量值自动进行调整。

选中 Spike Filter 复选框，并输入每秒通过的流量最大数值（单位为 Volume 字段所选值），则可避免由于发生错误而产生曲线图的高峰值图形，生成较为均衡的曲线图。

注意：设备性能类的监测对象（如内存利用率），其设置项略少于流量类的监测对象（如交换机端口速率），但设置内容基本类似。

（4）数据单位类型列表解释见表 10.1。

表 10.1　PRTG 可选数据单位描述

序　　号	类　　型	描　　述
1	Byte	字节，简写为 B，1 个 Byte 代表 1 个字元（A~Z）、数字（0~9）、符号
2	KB	千字节，1 KB= 1024 Bytes
3	megabyte	兆字节，简写为 MB，1 MB= 1024 KB
4	gigabyte	千兆字节，简写为 GB，1GB= 1024 MB
5	terabyte	太拉字节，简写为 TB，1TB=1024GB
6	bit	比特，一个二进制位，1Byte = 8bits
7	Kbit	千比特，1Kbit=1024bits
8	megabit	兆比特，1Mbit=1024Kbits
9	gigabit	千兆比特，1Gbit=1024Mbits
10	terabit	太拉比特，1Tbit=1024Gbits

10.1.5 节点配置——Billing 账单

在节点配置界面中选择 Billing 选项，进入账单配置界面，配置 PRTG 生成按流量计费的账单，如图 10-19 所示。

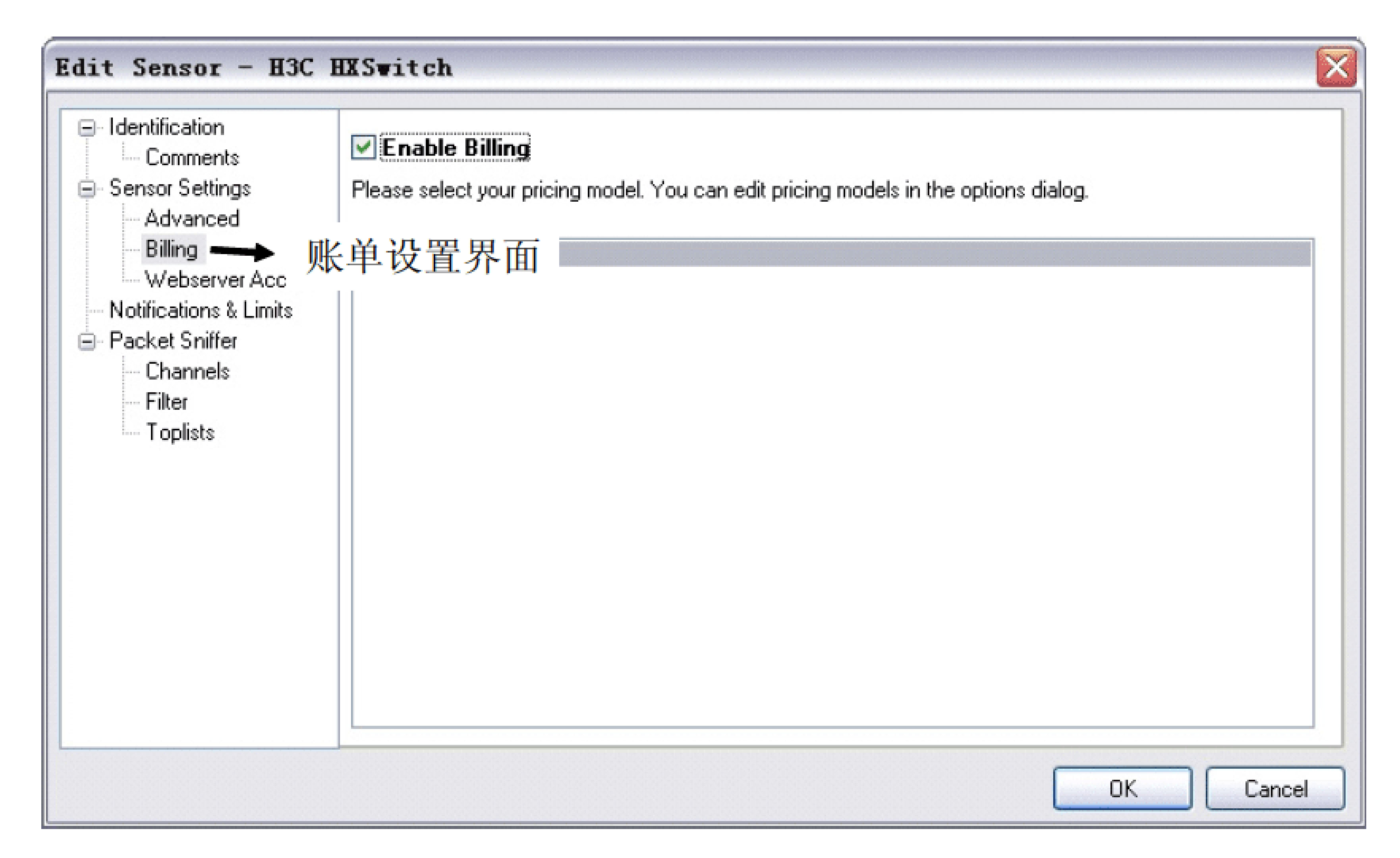


图 10-19 账单设置界面

该项配置对于需要按照接收数据总量进行付款的企业较为适用，配置计费模式后 PRTG 将按照计费方式生成账单。选择 Enable Billing 将开启对该节点的计费。但计费模式在主界面菜单命令 Extra | Options 界面中进行设置。

打开 Extra | Options 界面后，在属性界面中选择 Billing 选项，如图 10-20 所示。

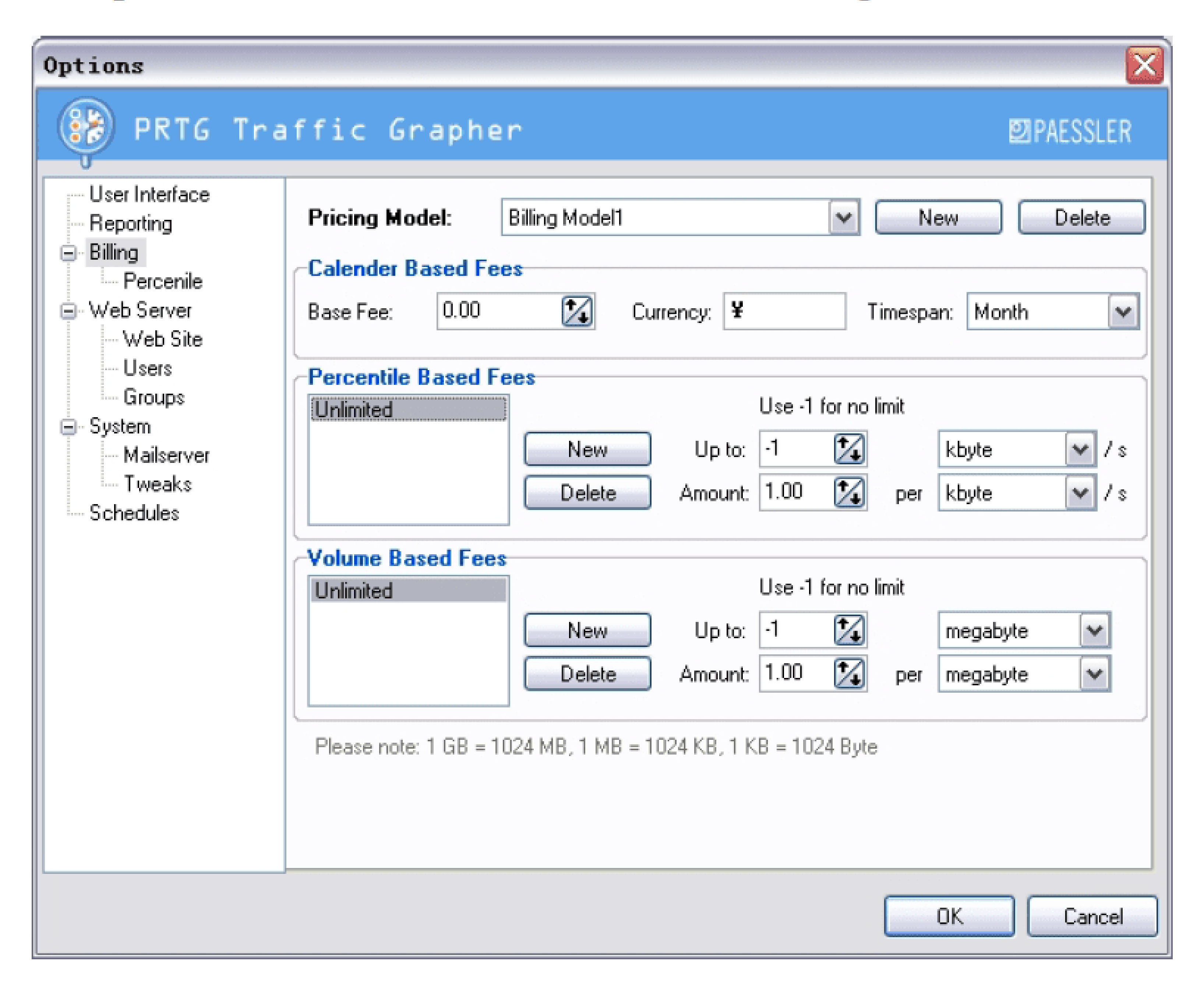


图 10-20 Billing 付费模式设置

该界面中提供了 3 种基本的定价。

- ❑ Base Fee：定义每个时间跨度内需要付款的数额，例如每月付款 40￥。
- ❑ Percentile Based Fees：按照带宽利用率情况付款方式，在设定基础费用后，在带宽利用率超过 95%的时长内，还需付额外的费用。该方式需要在 Billing | Percentile 选项页面进行设置。
- ❑ Volume Based Fees：按照超过容量值付款方式，例如设置每月免费接收或包月接收容量为 100G，每当超过 1G 容量后，再进行付款 0.5￥。

实例：建立一个每月可接收 100G 容量，月付费用为 40￥，当接收容量超过 100G 后，每增加 1G，则额外提供 2￥付费的付费模式。设置步骤如下：

（1）在 Pricing Model 项新建付费模式，并命名为 Billing Model。设置月付费用 40￥，在 Base Fee 选项中输入数值 40，时间跨度选择为 Month，如图 10-21 所示。

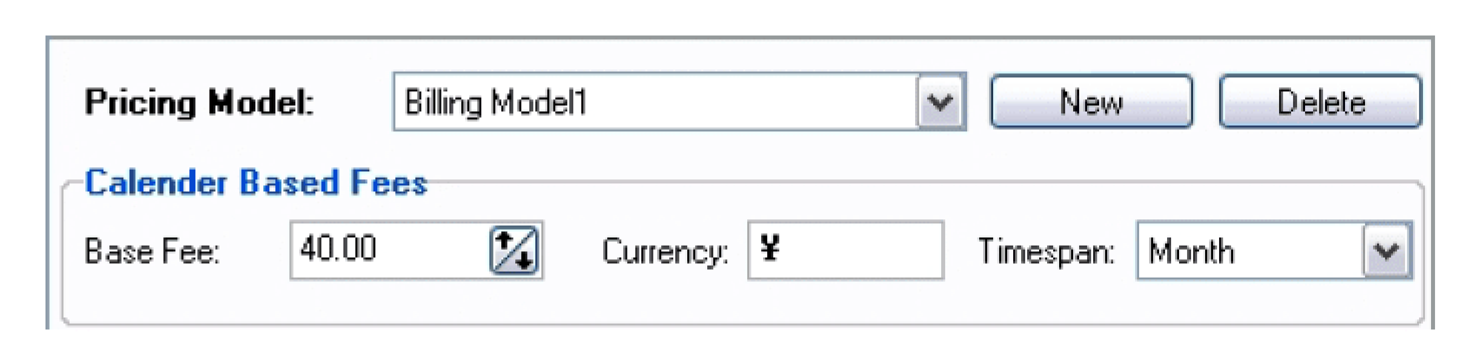


图 10-21 设置基础付费额

（2）设置基础接收容量为 100G。此模式下，不使用按百分比付款的模式，所以在 Percentile Based Fees 区域中设置 Amount 参数为 0，在 Volume Based Fees 区域中设置 Up to 内容为 100，单位选择为 gigabyte，更改 Amount 参数为 0，即接收容量达到 100G 为上限额度，如图 10-22 所示。

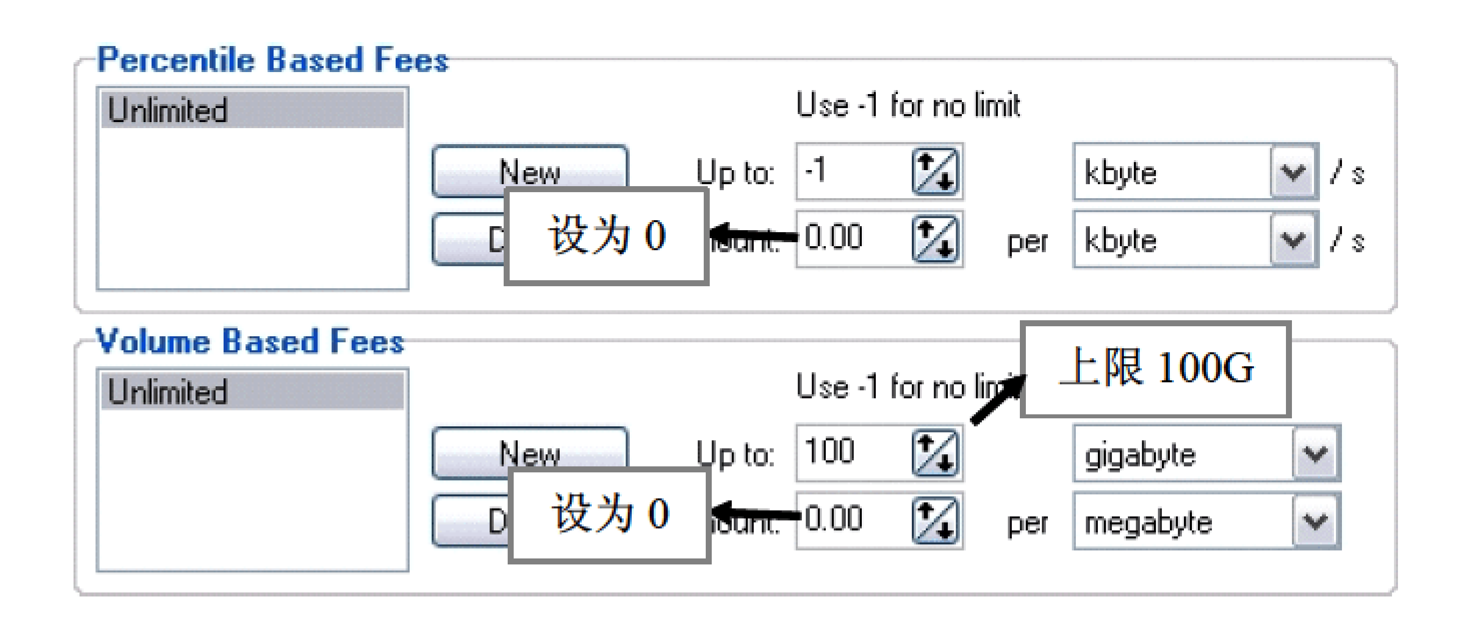


图 10-22 设置基础付费可接收容量上限

（3）设置每当递增 1G 容量，付费 0.5￥，在 Volume Based Fees 区域，需要建立一个递增付费项。选择 New，新建一个命名为 0.5￥ Per Gigabit 项，选择该项后，设置其 Up to 参数为–1，设置 Amount 项为 0.5，即每 G 则额外付费为 2￥，如图 10-23 所示。

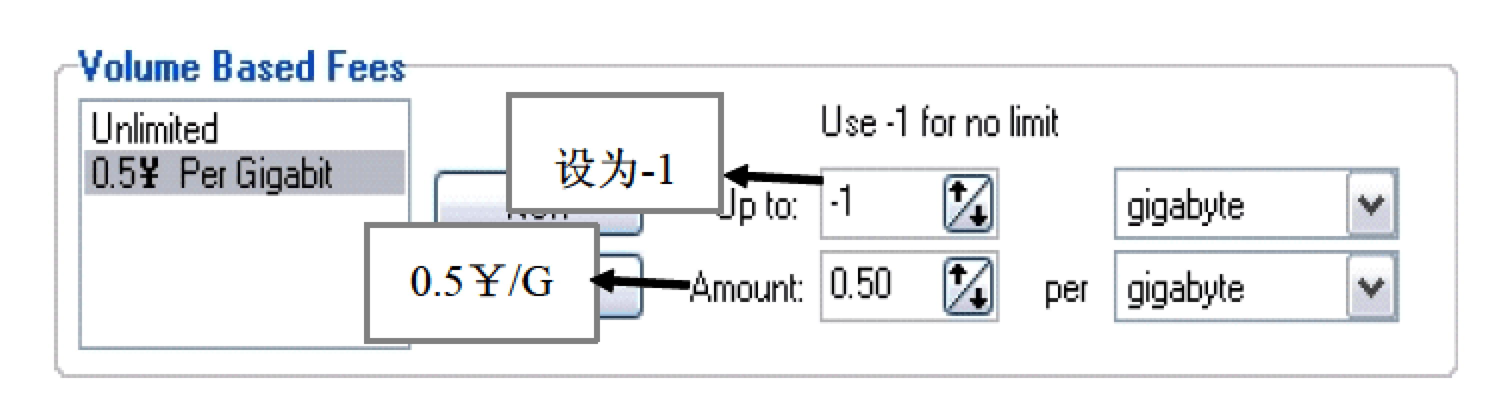


图 10-23 设置递增付费项目

设置完毕后，回到 Sensor Edit | Billing 设置界面，在列表中将看到刚才建立的账单模式，选中 Enable Billing 复选框，则对该节点启用账单计费，如图 10-24 所示。



图 10-24　选择并完成 Billing 账单设置

完成该项设置后，在生成该节点的报表时，只需要选中包含的账单选项，报表中将生成账单计费信息。

10.1.6　节点配置——PRTG Web 模式

节点配置界面中，选择 Webserver Access 选项，配置访问 PRTG Web 模式的账户信息，如图 10-25 所示。



图 10-25　配置访问 PRTG Web 界面的账户

该界面中，列出了可访问 PRTG Web 界面数据的账户或用户组，而用户组和账户信息在主界面菜单命令 Extra | Option 的设置界面中，选择 Web Server 选项进行配置，如图 10-26 所示：

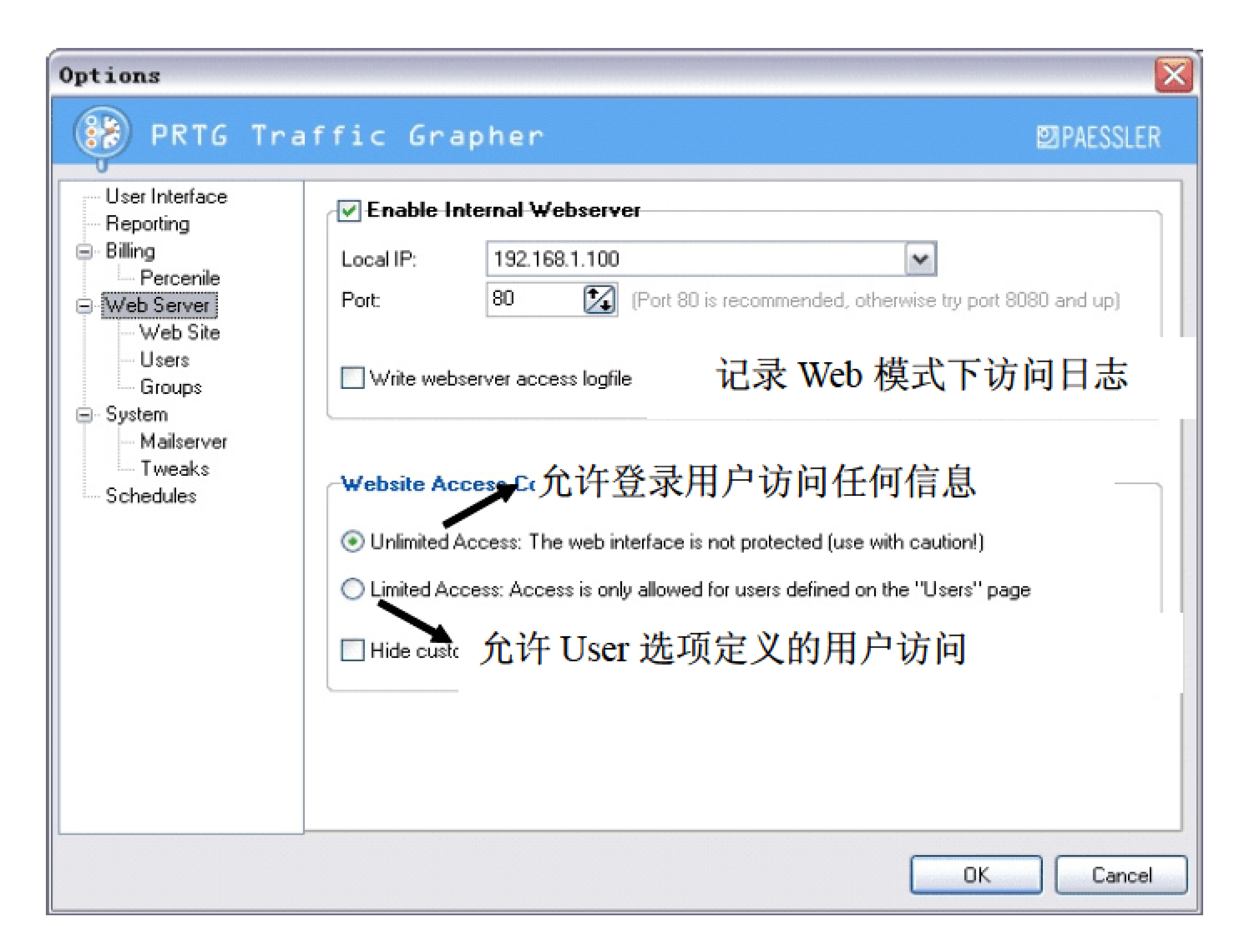


图 10-26　Web 界面设置

在如图 10-26 所示的界面中，可设置本地 IP 地址和端口（默认为 80，如被占用则使用 8080 或其他未使用的端口）。在网页中输入本地主机 IP 地址 http://127.0.0.1/sensorlist.htm 即可访问 PRTG Web 界面。选中 Write webserver access logfile 复选框，则 PRTG 会记录 Web 模式下用户访问数据的日志。在 Website Access Control 选项可设置允许登录用户访问所有数据或仅允许已添加的用户访问。

Web 模式的设置页面还包括 Web Site，用于设置 PRTG Web 模式的站点名、管理员 E-mail、网页配色方案、Web 模式界面大小等信息。Group 用于添加用户组，Users 页面用于添加、删除登录 PRTG Web 界面的账户名和密码等，如图 10-27 所示。

注意：添加的账户需要确保至少属于某一用户组，用户组的添加、删除在 Group 选项中进行管理。

10.1.7　节点配置——报警提示模式

在节点配置界面中，选择 Notification & Limits 选项，可配置报警提示模式。PRTG 在发现节点错误、达到阈值或达到指定容量时会发出提示信息。默认 PRTG 为每个节点自动生成一个错误提示，当发生错误时，该节点背景色显示为粉红色。PRTG 共支持 4 种类型的提示。

- Error Notifications：节点错误提示；
- Threshold Notifications：到达指定阈值提示；

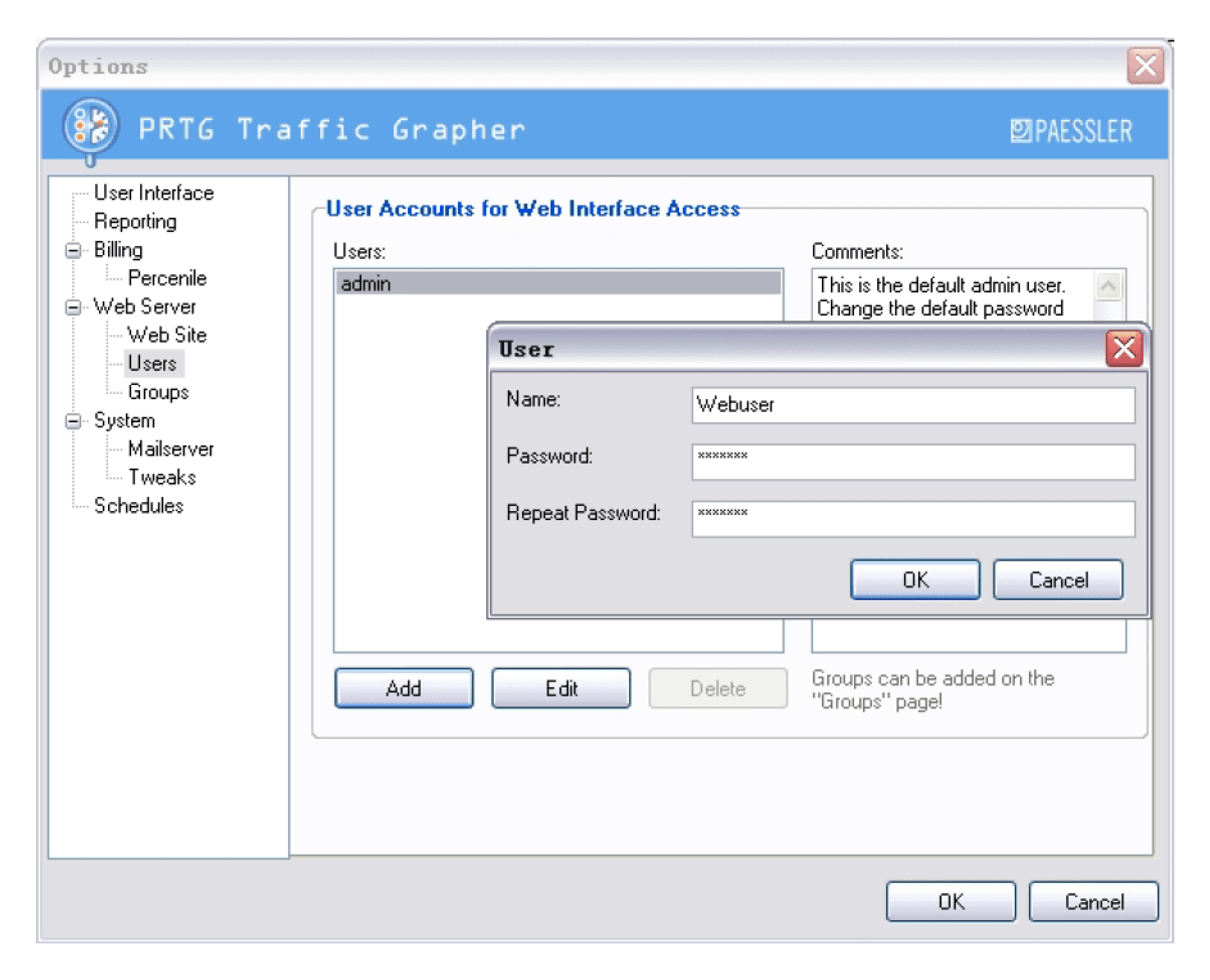


图 10-27　添加登录 PRTG Web 界面账户

- ❑ Volume Notifications：达到指定容量提示；
- ❑ Limit Line：流量到达限定速率时，将在曲线图中添加一条水平的提示线作为提示。

报警提示设置界面如图 10-28 所示。



图 10-28　设置告警提示

以下对 PRTG 支持的 4 种告警提示方式做详解。

方式 1：单击 Error Notifications 按钮，打开节点错误提示界面，如图 10-29 所示。

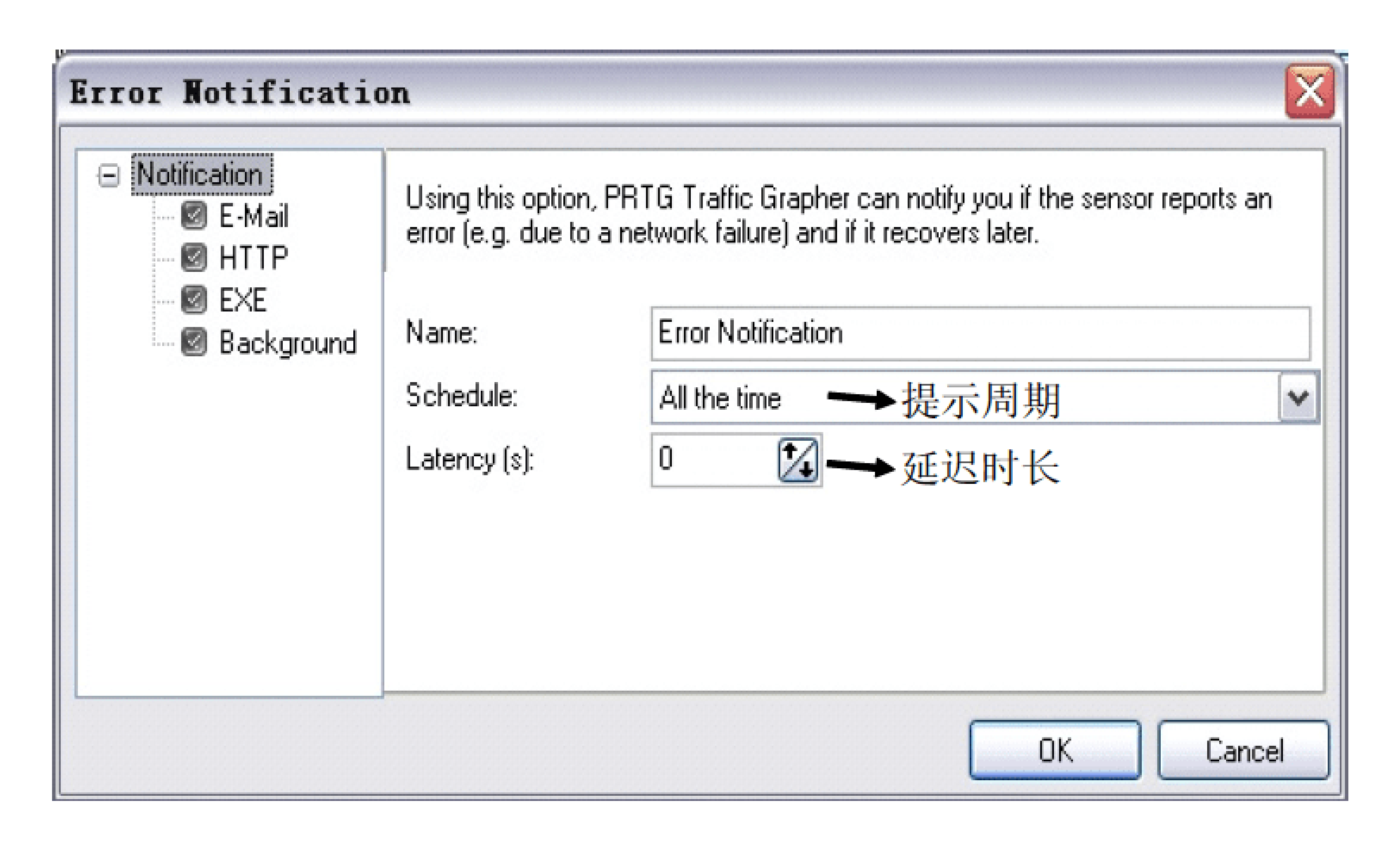


图 10-29　添加错误提示

在图 10-29 所示的界面中可设置新建错误提示的名称；Schedule 选项可更改 PRTG 发送错误提示的时间周期；设置 Latency 可增加发送错误提示的延迟时间，在发生突然性错误时，允许 PRTG 在延迟时间内修复错误，如果恢复正常运行，则不进行告警提示。

方式 2：在 Notification & Limits 界面，单击 Threshold Notifications 按钮，打开达到指定阈值提示设置界面，如图 10-30 所示。

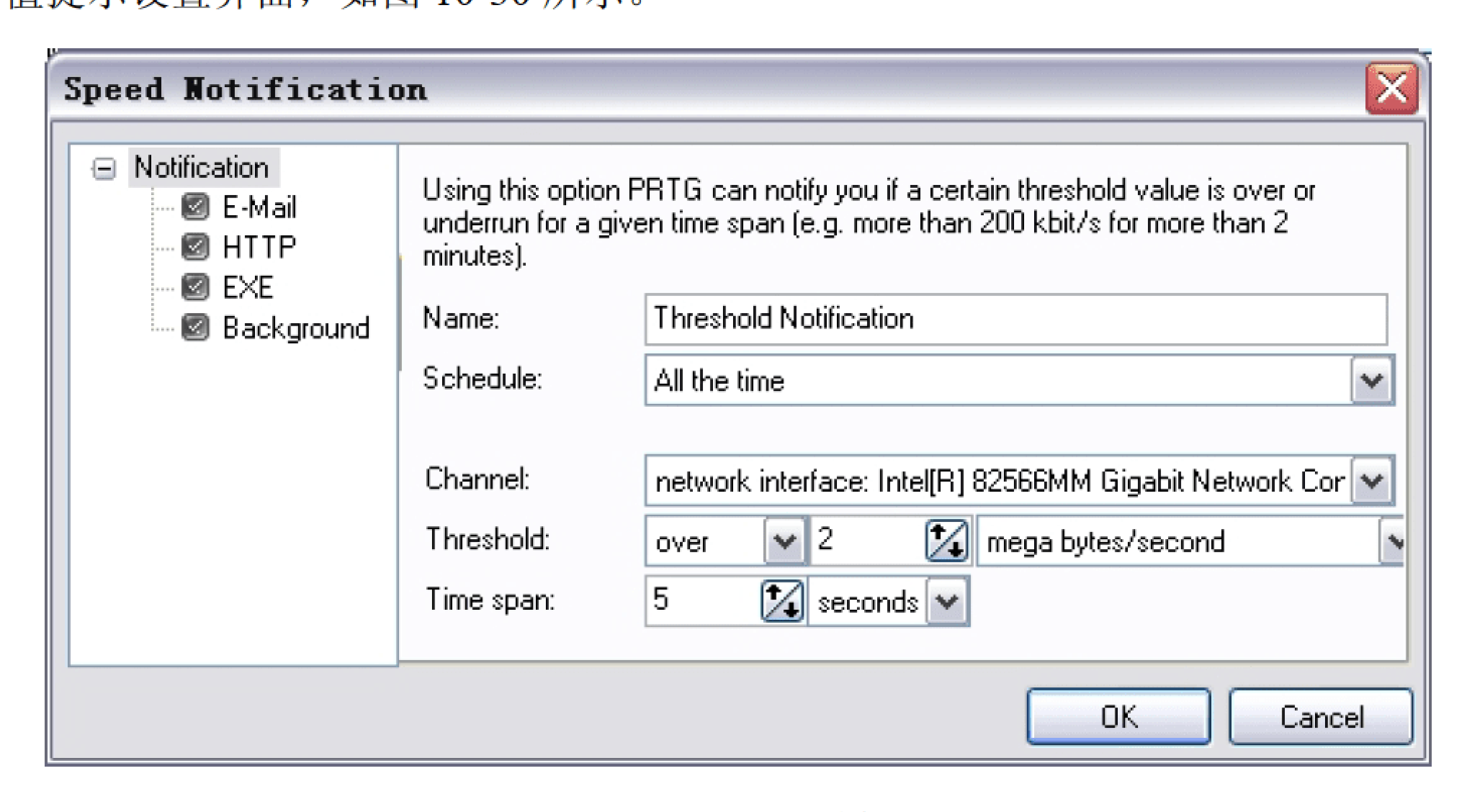


图 10-30　设置阈值提示

在图 10-30 所示的界面中，可设置新增阈值提醒的名称、时间周期；Channel 在针对不同类型节点时选项不同，例如可选择流进、流出、合计阈值或各类协议等通道；更改 Threshold 阈值项，可配置发出提示的阈值。此处设置的数据为在时间跨度为 5 秒内，流经本地网络的速率超过每秒 2Mbyte 时，发出告警提示信息。

注意：确保此处设置的时间跨度值 Time Span 必须大于为该节点设置的轮询时间周期。

方式 3：在 Notification & Limits 界面，单击 Volume Notifications 按钮，打开达到指定

容量提示设置界面，如图 10-31 所示。

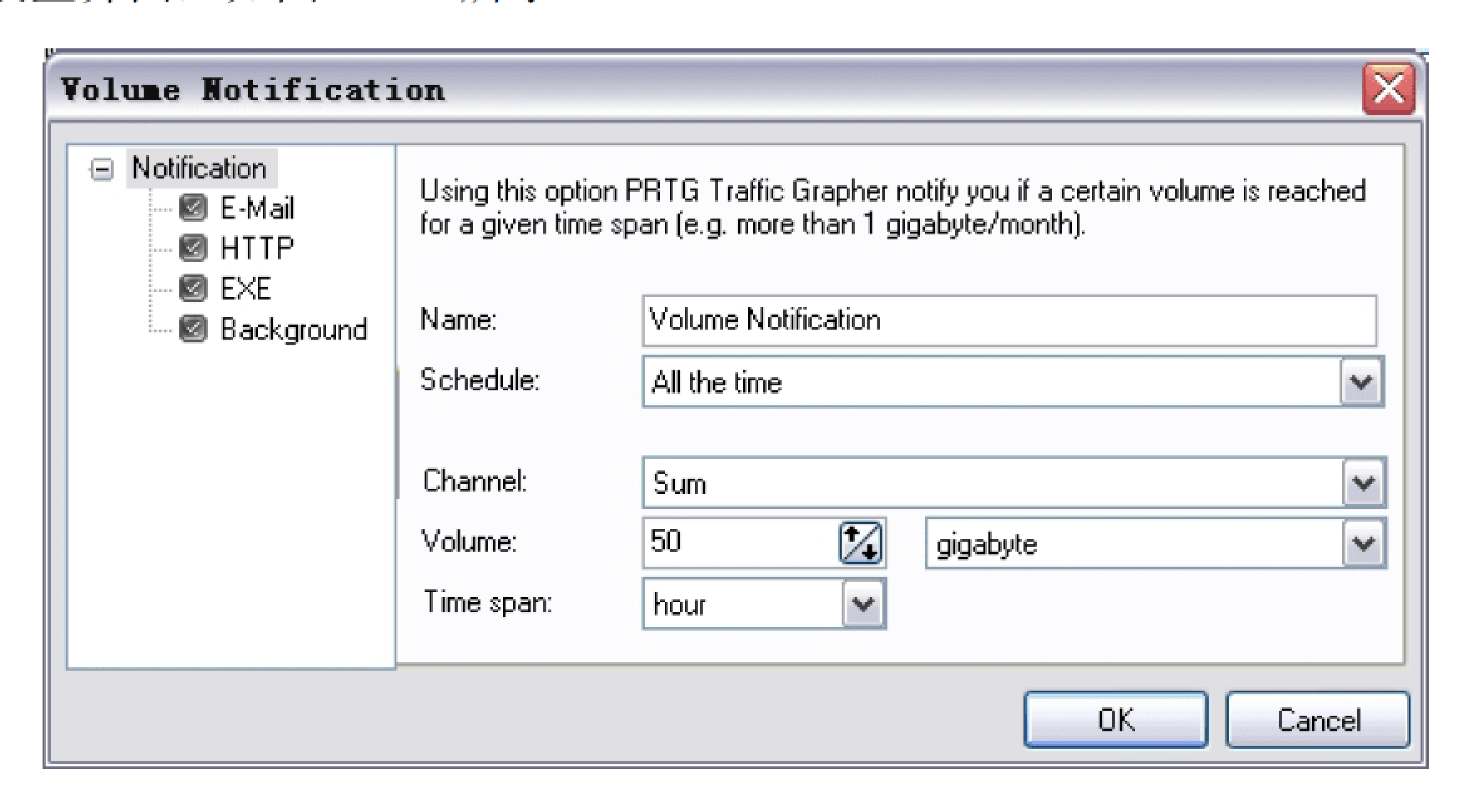


图 10-31　设置达到容量提示

在如图 10-31 所示的界面中，可设置新增容量提示的名称、时间周期及用于统计的数据通道；更改 Volume 项，可配置发出告警提示的容量限制。此处设置为在时间跨度为 1 小时内，进入节点端口的数据总容量超过 50GB，则发出告警提示信息。

方式 4：在 Notification & Limits 界面，单击 Limit Lines 按钮，打开添加水平提示线界面。当流量达到指定速率时，将在曲线图中自动添加一条水平的提示线，如图 10-32 所示。

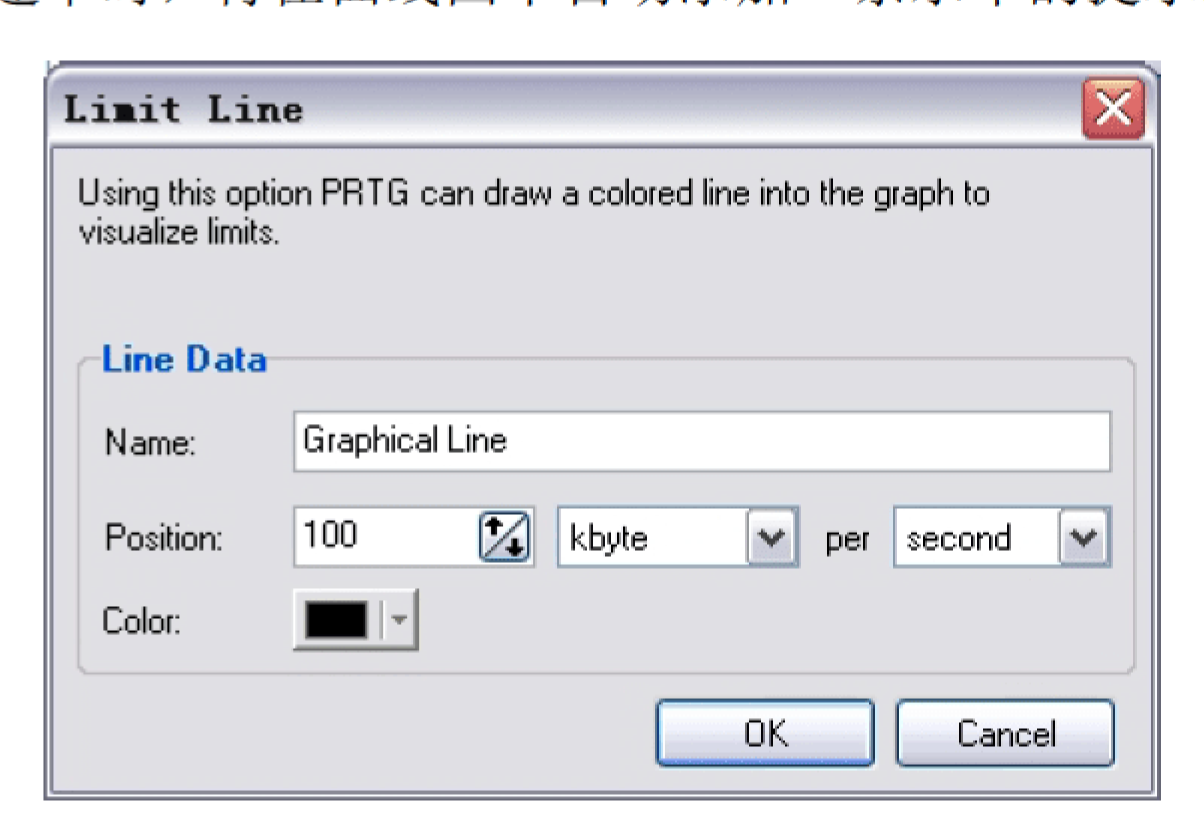


图 10-32　添加水平提示线

10.1.8　节点配置——报警提示动作

介绍完报警方式后，接下来介绍发生报警时 PRTG 执行的提示动作。PRTG 在进行报警提示时，可通过 4 种动作展现提示信息，即发送 E-mail、发送 HTTP 请求、执行外部 exe 文件或批处理文件、改变节点的背景显示颜色。下面对 4 种提示动作做详解。

动作 1：添加发送 E-mail 的提示动作，如图 10-33 所示。

设置通过 E-mail 发送提示信息，需要输入接收邮件 E-mail 地址及 E-mail 模板。同时，还需要在 PRTG 主界面的菜单 Extra | Options 界面中配置邮件服务器，该功能才能正常启用，

在 Options 界面中选择 System | Mailserver 选项，如图 10-34 所示。

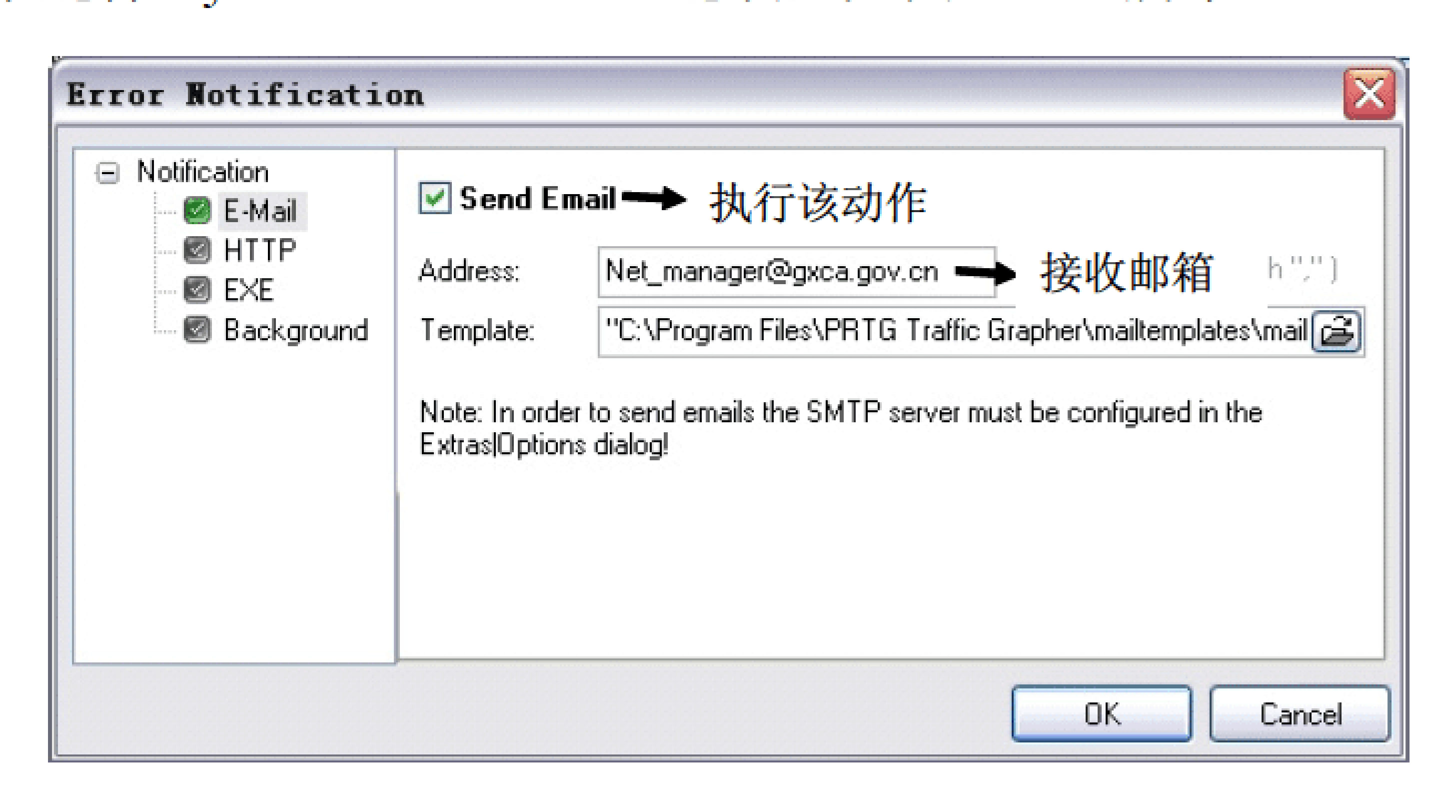


图 10-33　发送 E-mail 提示配置

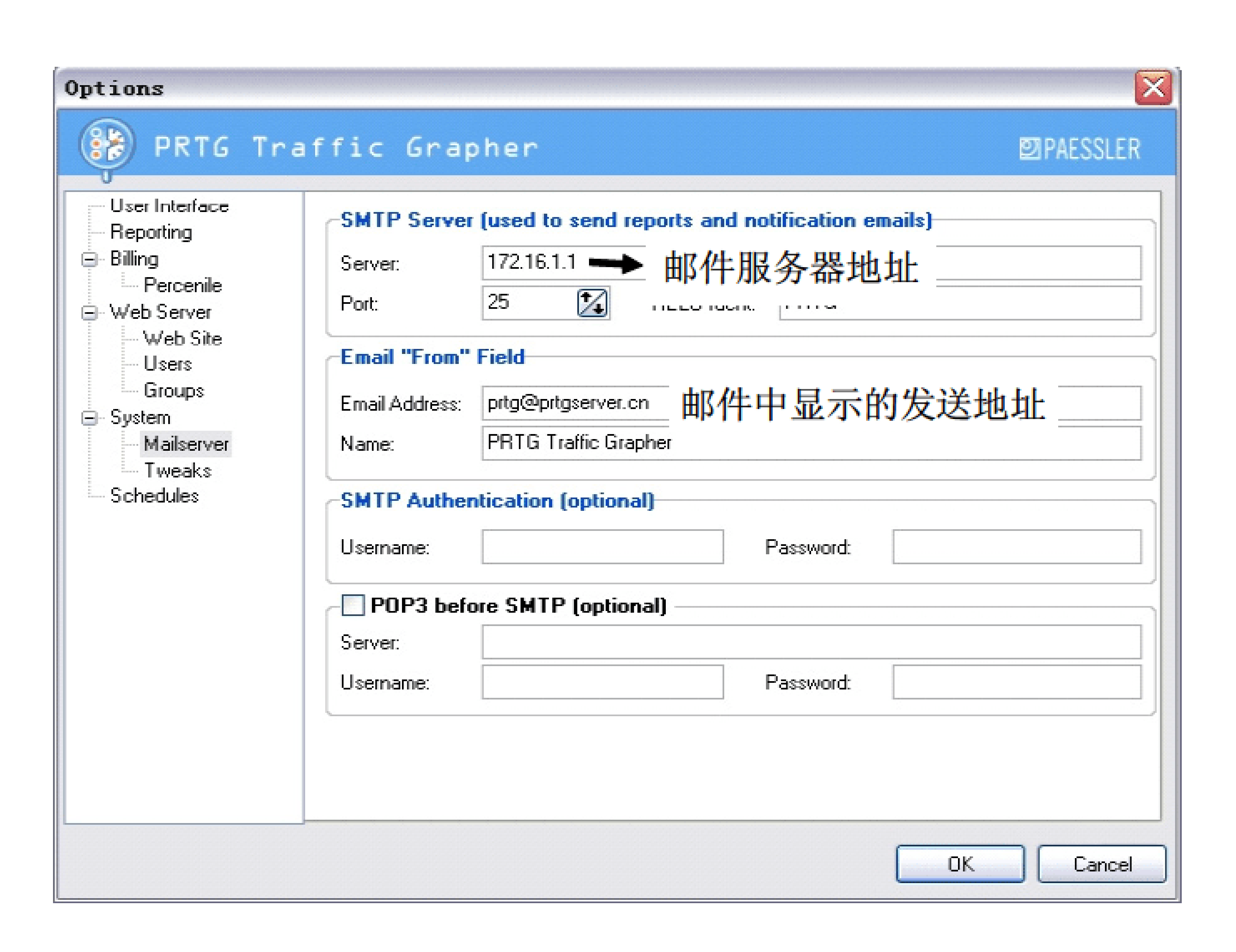


图 10-34　设置发送邮件提醒的邮件服务器

在邮件服务器设置界面中，输入服务器的 IP 地址，在 E-mail From Field 中可输入发送者的地址，该地址将在邮件中的发送者位置显示；同时，需要输入登录邮件服务器的账号和密码，如果邮件服务器还需要 POP3 账号，则同样需要输入用户名和密码。

为节点配置 Email 提示动作后，可接收到来自节点的邮件，如图 10-35 所示。



图 10-35　接收到的 E-mail 提示信息

邮件的内容样式及包含的信息如图 10-36 所示。



图 10-36　接收到的提示邮件包含的信息

动作 2：添加执行 HTTP 请求动作，设置 HTTP 链接地址，PRTG 会向链接发送 HTTP 请求。

动作 3：添加执行外部 exe 文件或批处理文件动作。当 PRTG 出现报警提示时，将调用设定的外部 exe 文件或批处理文件。

动作 4：添加改变 PRTG 故障节点背景颜色的动作，如图 10-37 所示。

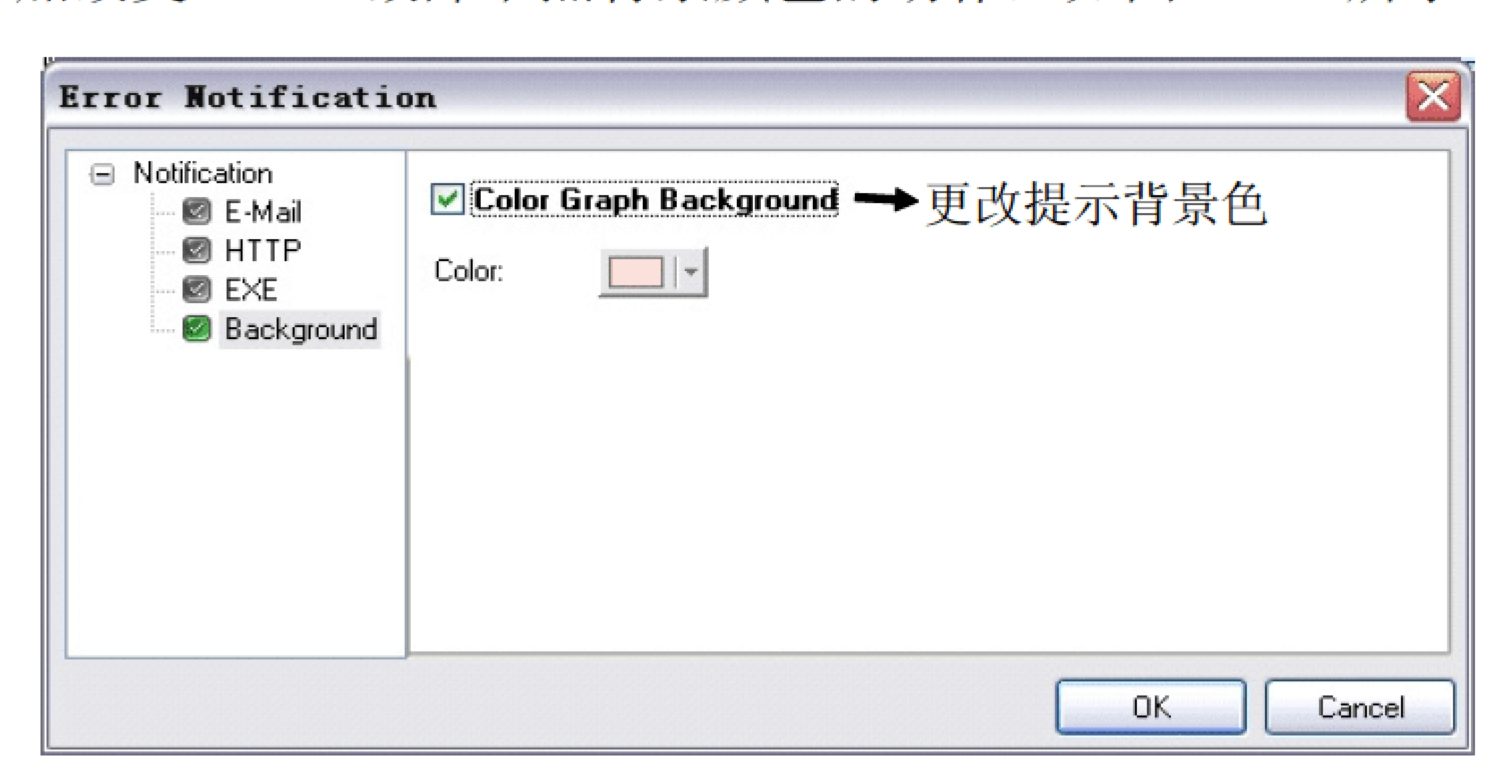


图 10-37　改变故障节点背景颜色设置

注意：如果需要执行以上 4 种动作中的某项动作，需要选中该动作的复选框。例如，在图 10-21 中选中 Color Graph Background 复选框。

10.1.9　节点配置——SNMP 属性

如果所选节点是 SNMP 方式的监测节点，则在 Edit 界面中显示的是 SNMP 设置项，如图 10-38 所示。

在图 10-38 所示的界面中，可设置 SNMP 版本，通常使用 V1 和 V2 版本，还可以设置该节点的显示名、IP 地址、访问端口和社区字符串。

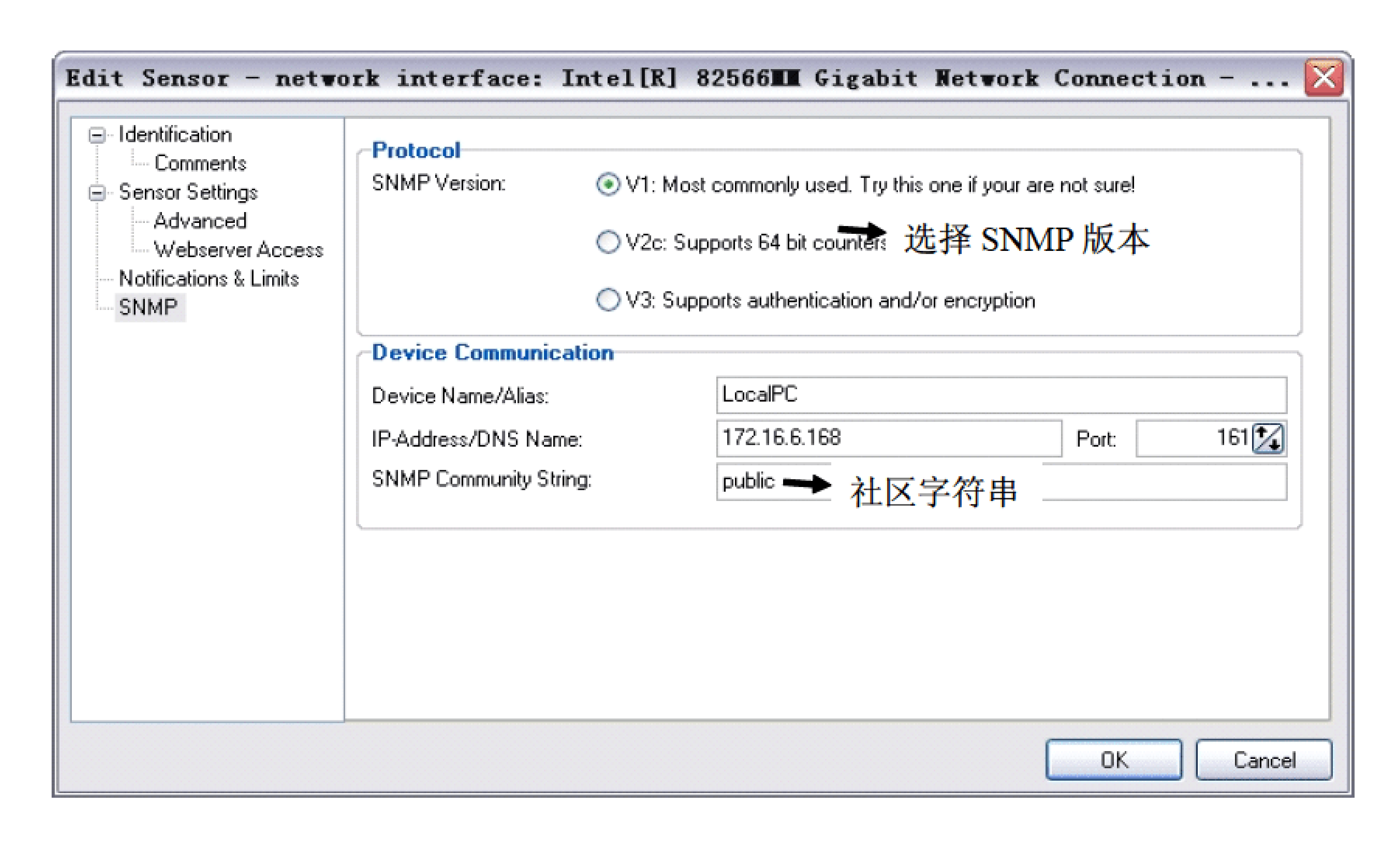


图 10-38　设置 SNMP 属性

如果 SNMP 设置项目中包含 Channels 选项（如图 10-39 所示），则可设置要监测的数据通道。选中合计、流入数据和流出数据 3 个复选框后，在实时监测曲线图中，会通过 3 种不同的颜色展现该 3 个通道的流量。

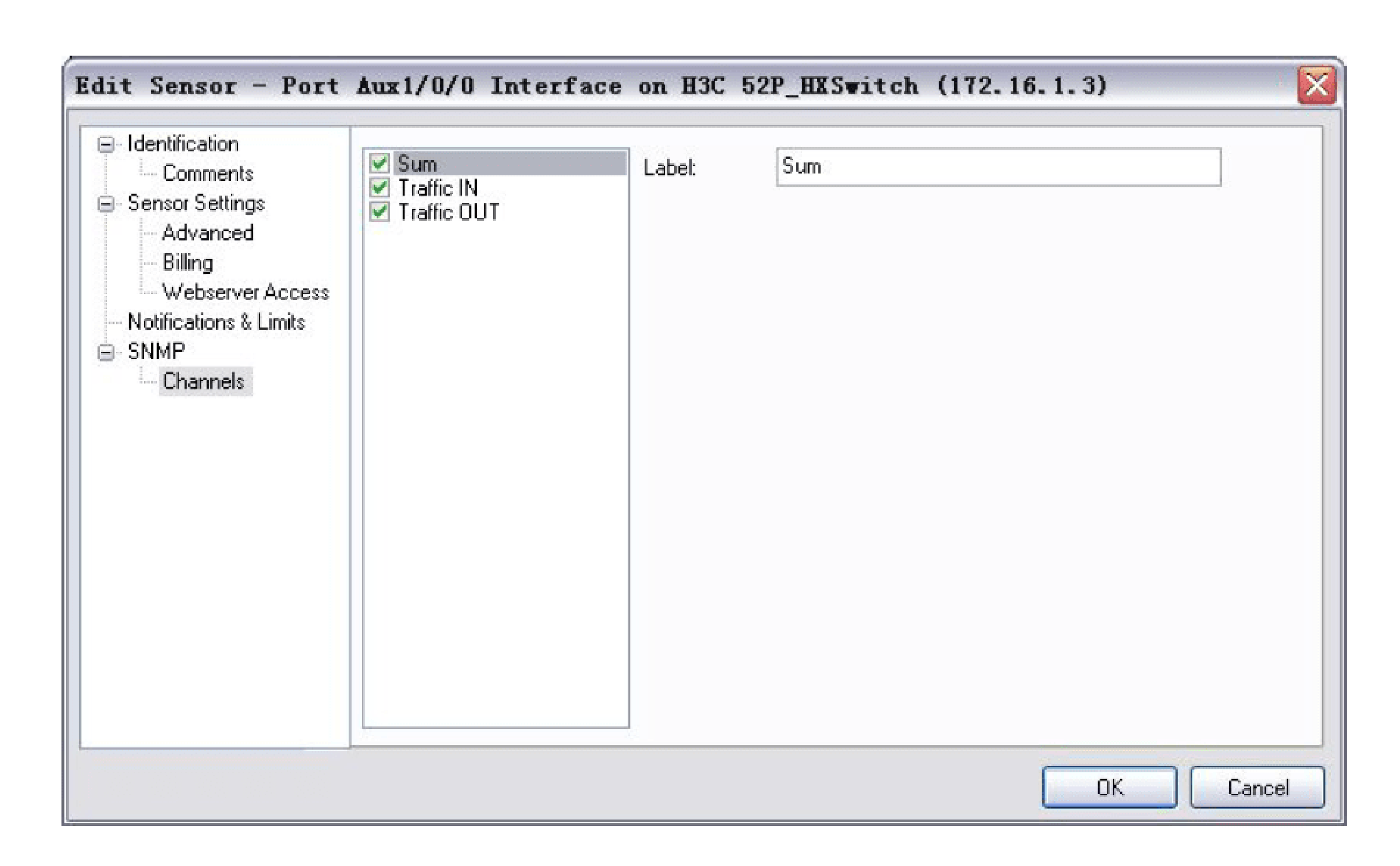


图 10-39　设置 SNMP 属性的 Channel 属性

如果所选节点是包探测方式监测节点，那么在 Edit 界面中显示的是 Packet Sniffer 设置项，如图 10-40 所示。

在图 10-40 所示的界面中包含 3 个设置项：Channel（数据通道）、过滤方式 Filter 和 Toplists 数据列表。数据通道用于选择要监测的协议对象；过滤设置用于选择需要包含的监

测内容和排除监测内容；Toplists 数据用于选择需要生成的节点信息。

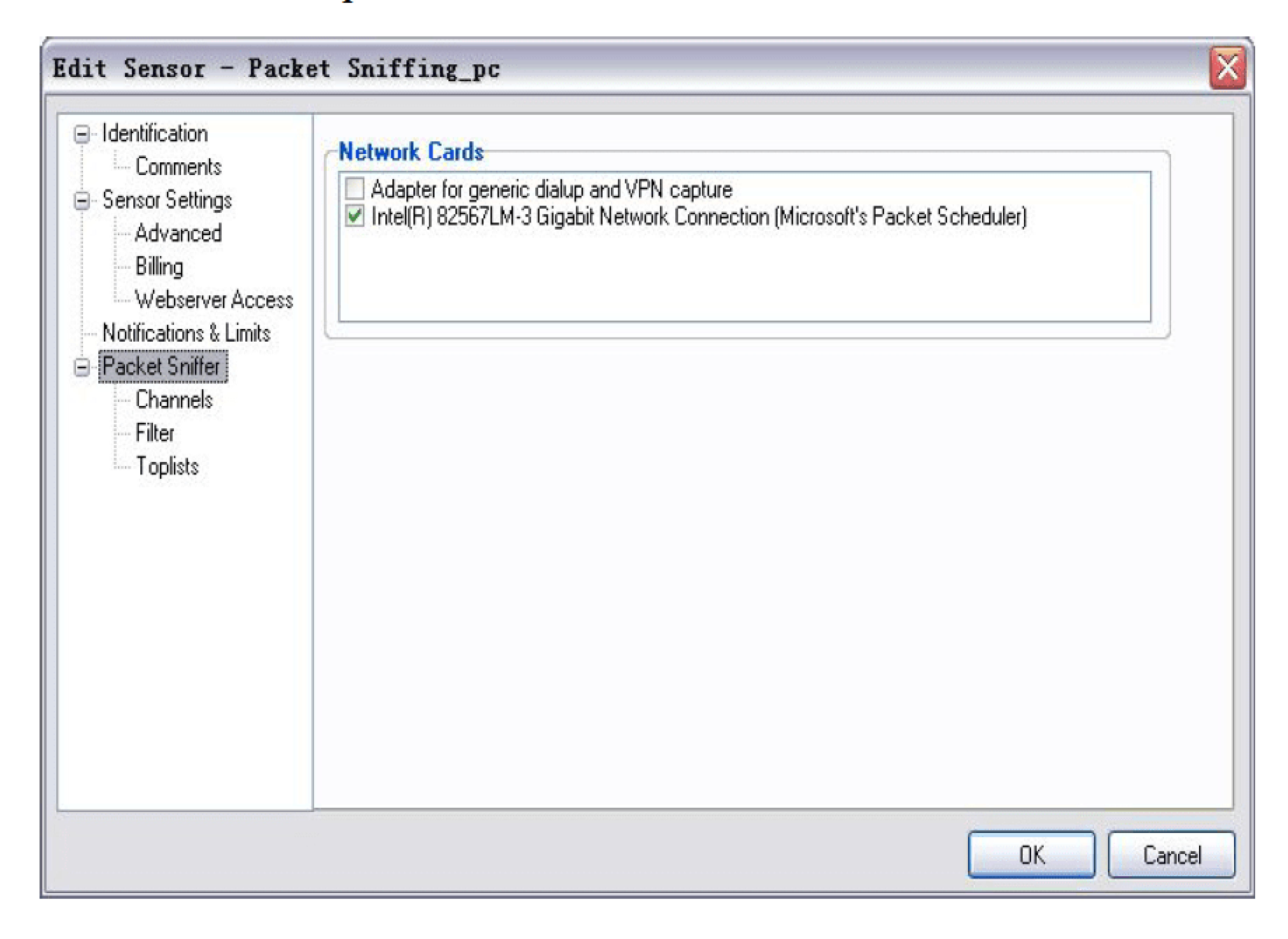


图 10-40　包探测方式可设置属性

其中，在 Toplists 设置界面，可选择的选项包括 Top Talkers（最活跃的目的 IP 地址排行）、Top Connections（两个设备间连接最活跃的排行）、Top Protocols（按最活跃的协议排行）。

10.2　用户自定义、报表和 Web 视图

10.2.1　Custom 用户自定义视图

在 Custom 视图中包含各种数据显示面版，可根据需要自定义图表和数据表的显示样式。同时，在面板中添加显示的图表和数据，能够在 Web 界面中展示。

选择 Views | Custom 命令进入设置窗口。如果是第一次使用该视图，可通过向导新建显示面板，也可按照窗口上方的导航控制条来添加，导航条提供了新增、删除、修改和排序视图面板功能，如图 10-41 所示。



图 10-41　Panel 导航控制条

在控制条中单击 Add 按钮，则弹出新建面板 Panel 配置窗口。在 Data 页面中，可输入

该面板的名称，以及是否允许在 Web 界面展示等；在 Layout 页面中，可选择面板样式，如果选择将面板样式（如图 10-42 所示）；备注页面 Comments 用于输入备注信息。

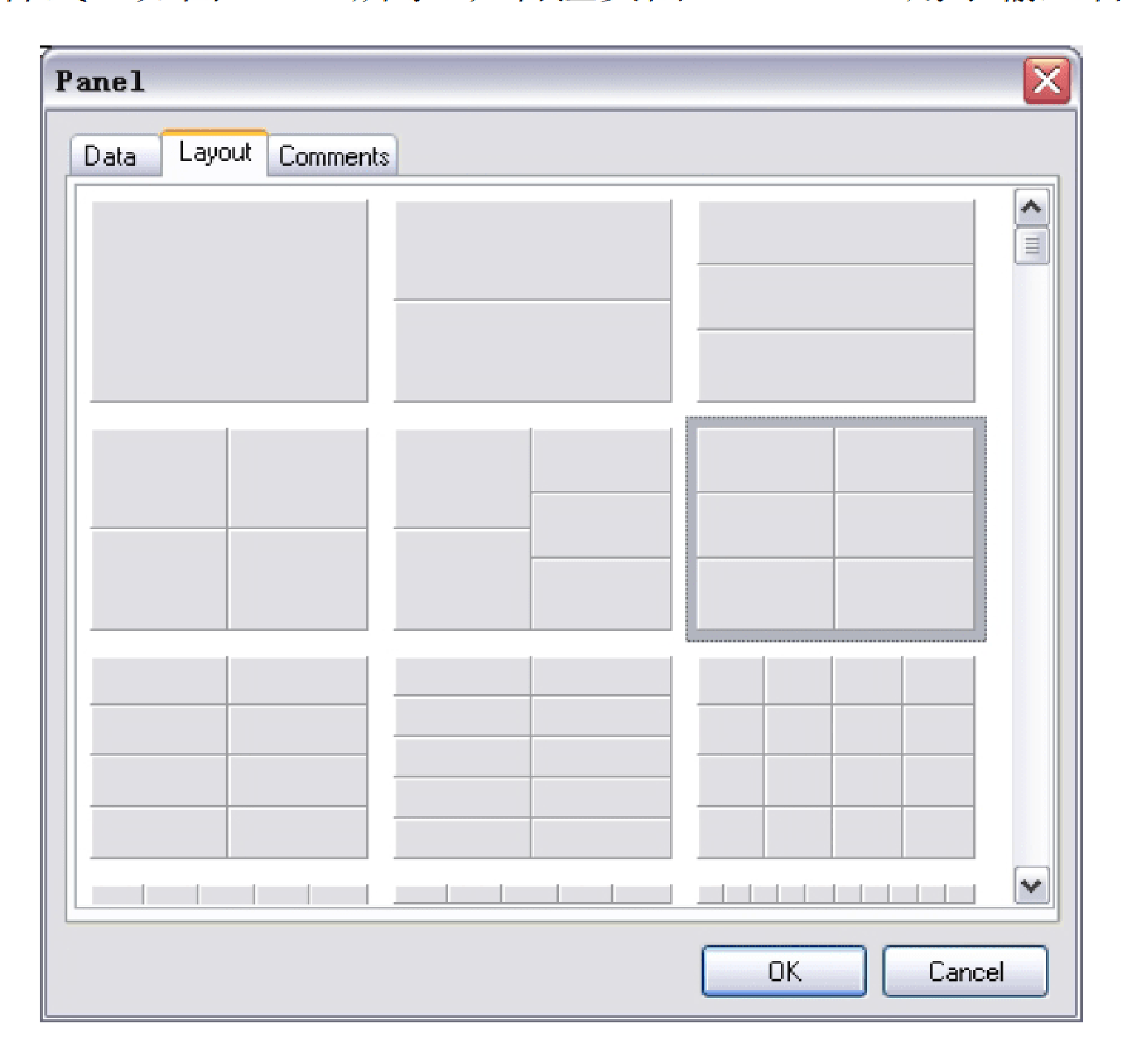


图 10-42　自定义图表模版选择

新建自定义显示面板步骤如下：

（1）选择面板样式后，单击 OK 按钮进入显示区域内容的添加，可选添加的对象包括 Graph（曲线图标）、Table（数据表）、Toplist（Top 数据表）3 种类型，如图 10-43 所示。

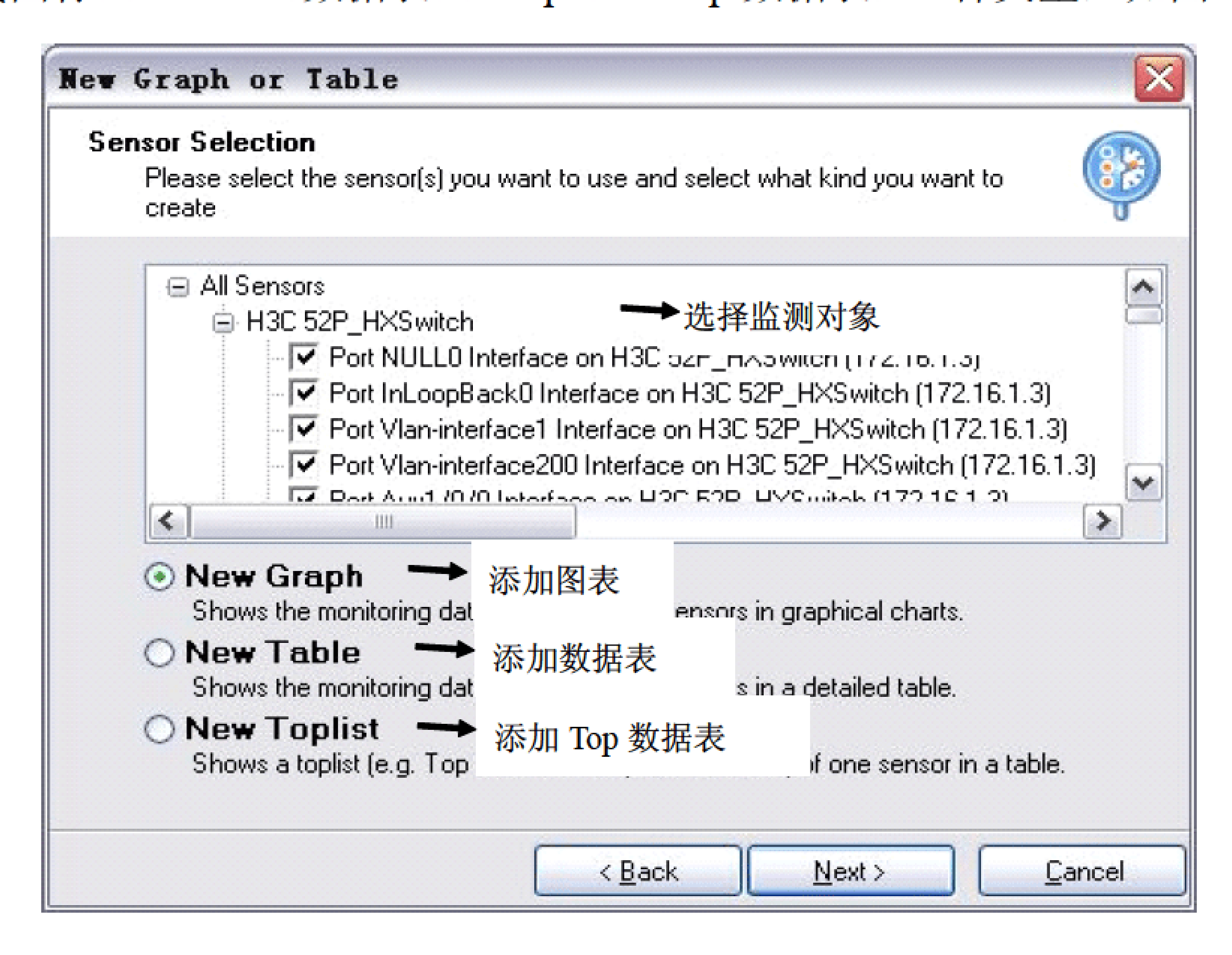


图 10-43　选择监测对象和显示数据的方式

（2）此处选择建立 New Graph，并进入下一步设置时间跨度。默认将包括 4 类时间跨度的曲线图，包括前 60 分钟实时流量、前 24 小时内 5 分钟流量的平均值曲线图等。界面如图 10-44 所示。

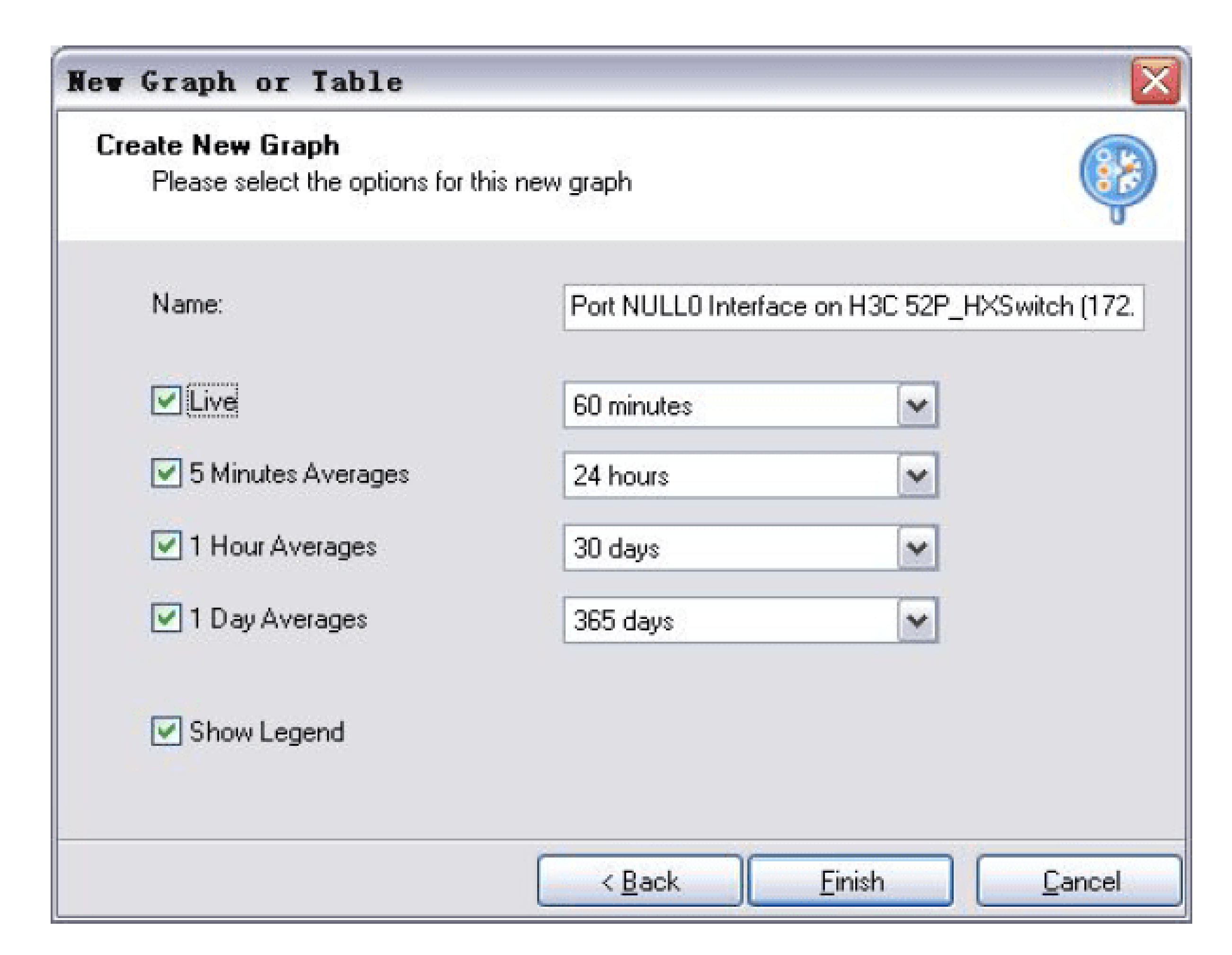


图 10-44　配置界面显示曲线图的时间跨度

注意：选择了 4 类曲线图，由于显示区域较小，面板中只显示前 60 分钟实时曲线图。双击曲线图放大图表后，在各个分页界面中可看到其他类型的曲线图。

（3）重复以上步骤，为面板中的其他显示区域添加上图表或数据表，直到完成自定义面板配置，如图 10-45 所示。

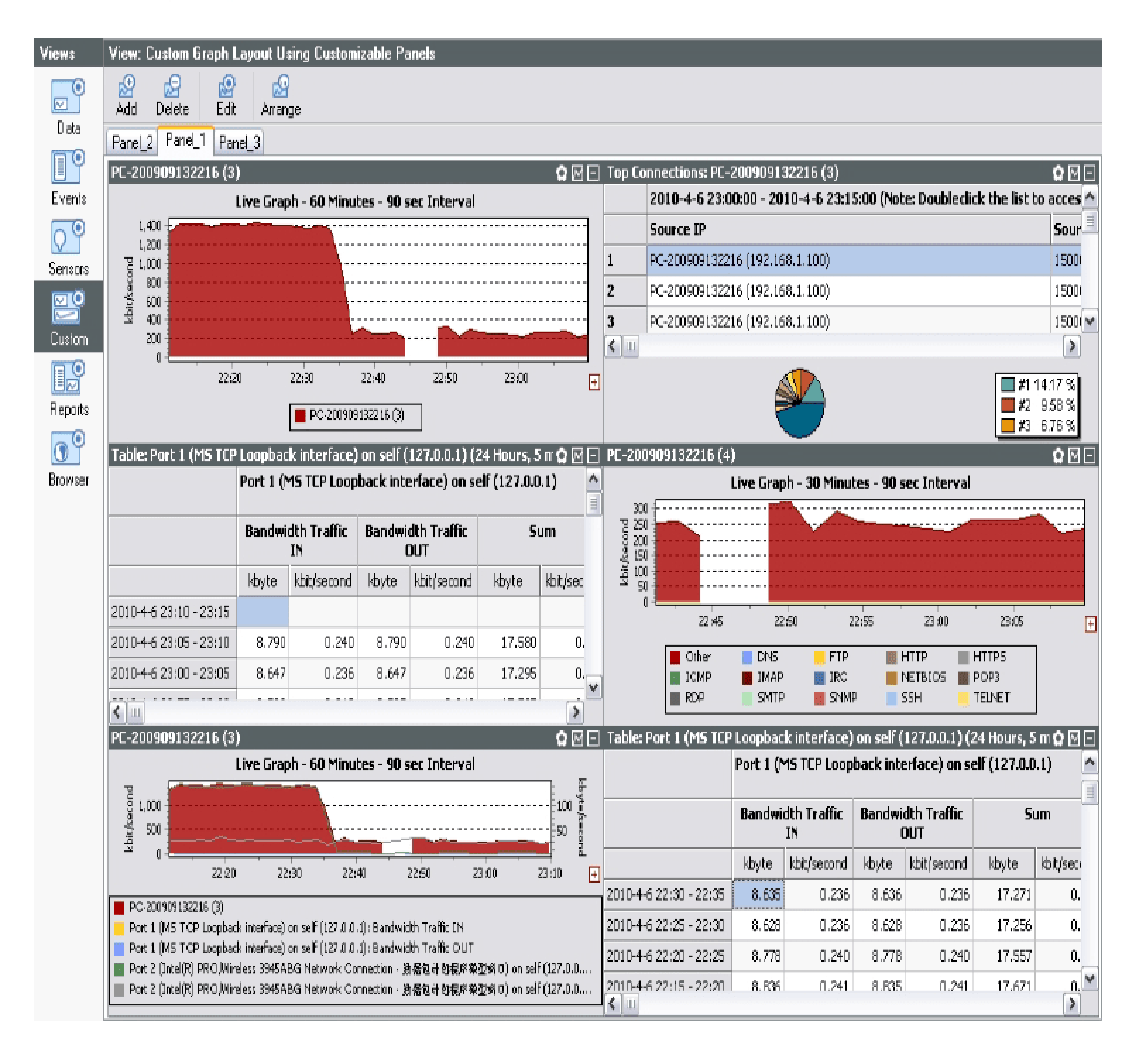


图 10-45　自定义 Panel 完成后显示的界面

10-47 所示。

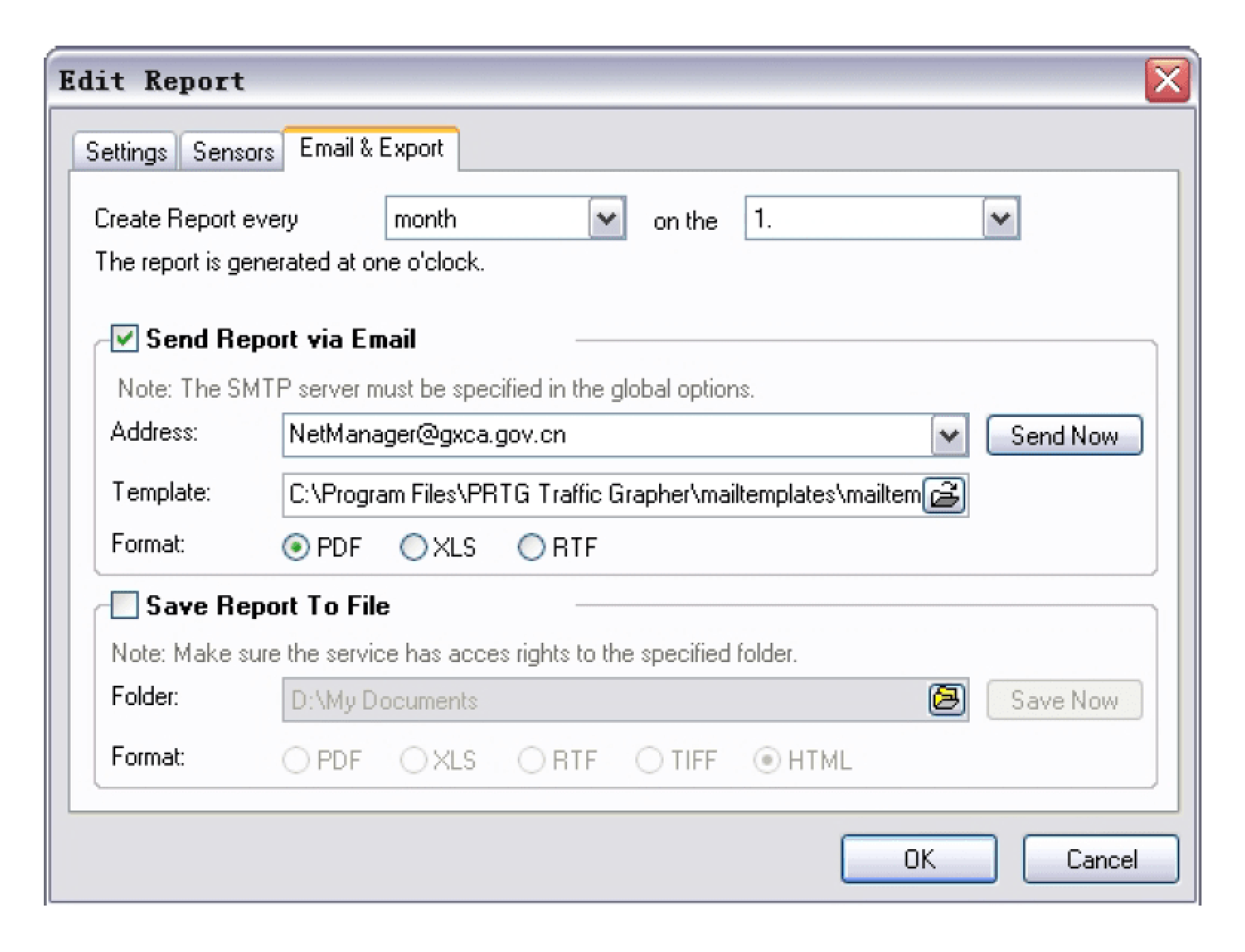


图 10-47 设置报表发送和保存的方式

2. 查看报表

新建报表后，将在 Report 视图中生成一条报表记录，双击某记录并选择生成报表的时间范围，如图 10-48 所示。

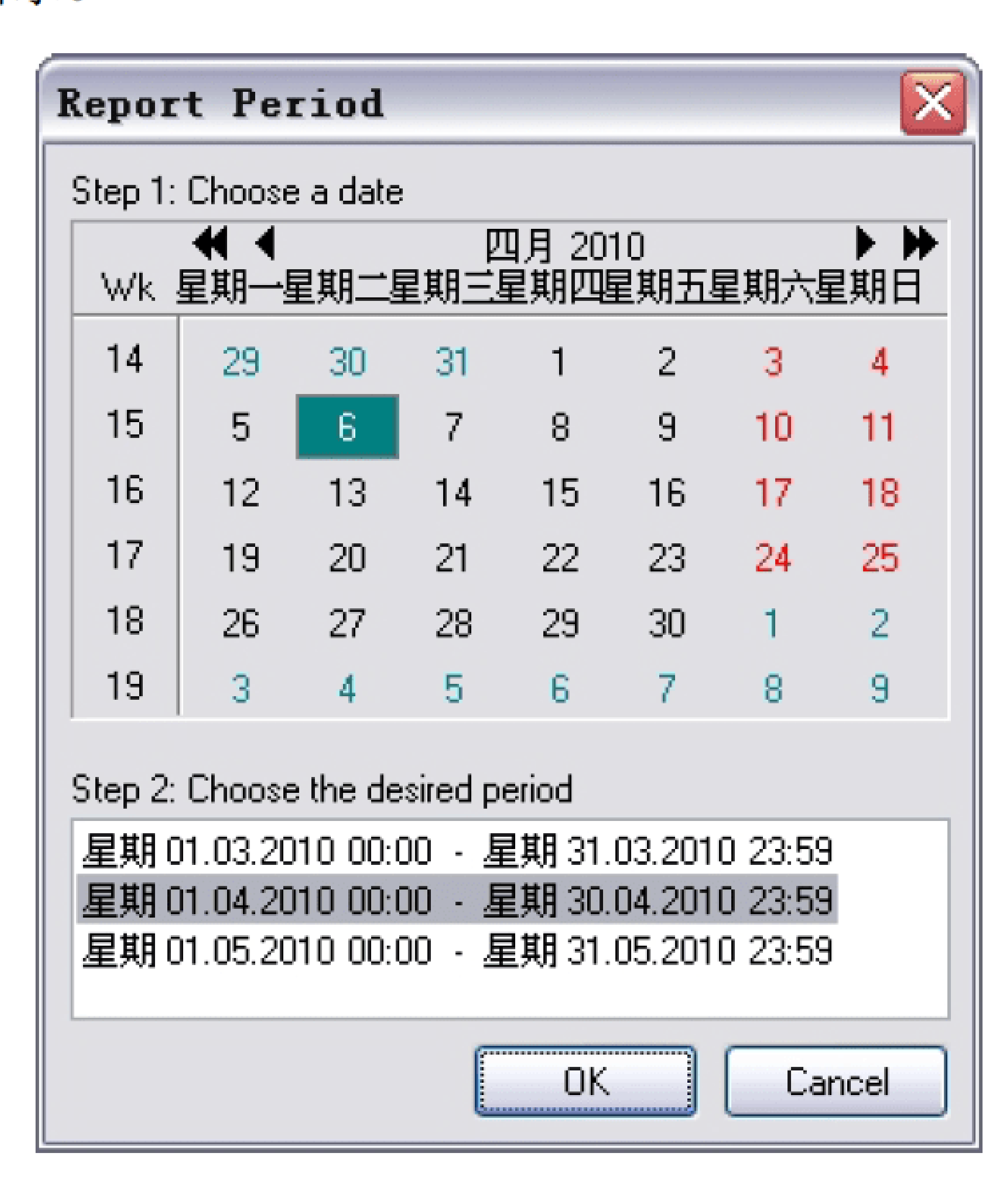
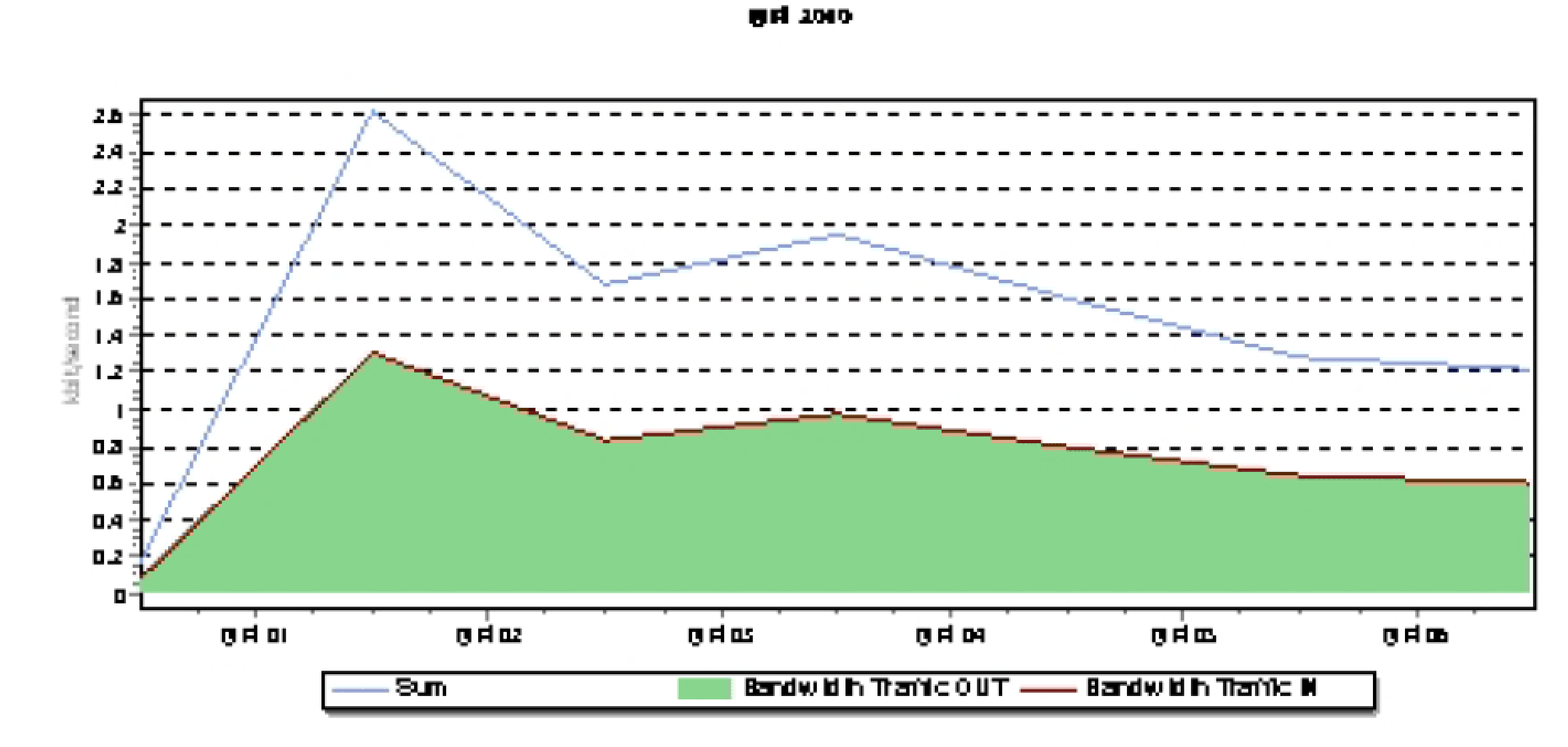


图 10-48 选择报表生成的时间范围

选择时间范围后，单击 OK 按钮，将生成详细的报表内容，如图 10-49 所示。

在报表界面中打开右键菜单，可将报表导出为多种格式，包括 PDF 文件、Html 文件等，如图 10-50 所示。





	Bandwidth Traffic IN			Bandwidth Traffic OUT			Sum			Coverage
	Kbyte	Kbit/second	95thPerc. (5 min)	Kbyte	Kbit/second	95thPerc. (5 min)	Kbyte	Kbit/second	95thPerc. (5 min)	%
2010-4-6	956.863	0.606	3.595	956.867	0.606	3.595	1,913.730	1.213	5.189	15
2010-4-5	3,115.664	0.644	4.331	3,115.660	0.644	4.331	6,231.324	1.288	8.661	46
2010-4-4	3,075.335	0.799	4.184	3,072.063	0.800	4.180	6,147.398	1.599	8.367	36
2010-4-3	4,809.564	0.975	4.271	4,809.566	0.975	4.271	9,679.131	1.951	8.543	47
2010-4-2	1,521.686	0.837	5.380	1,521.680	0.837	5.380	3,043.367	1.675	10.766	17
2010-4-1	525.521	1.307	5.309	525.521	1.307	5.309	1,051.043	2.614	10.618	4

Summary

	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum		Coverage
	Kbyte	Kbit/second	Kbyte	Kbit/second	Kbyte	Kbit/second	%
Total Volume	14,034.633		14,031.361		28,065.994		
Average		0.861		0.862		1.723	6
95thPerc. (5 min)		4.421		4.421		8.843	

图 10-49　报表示例

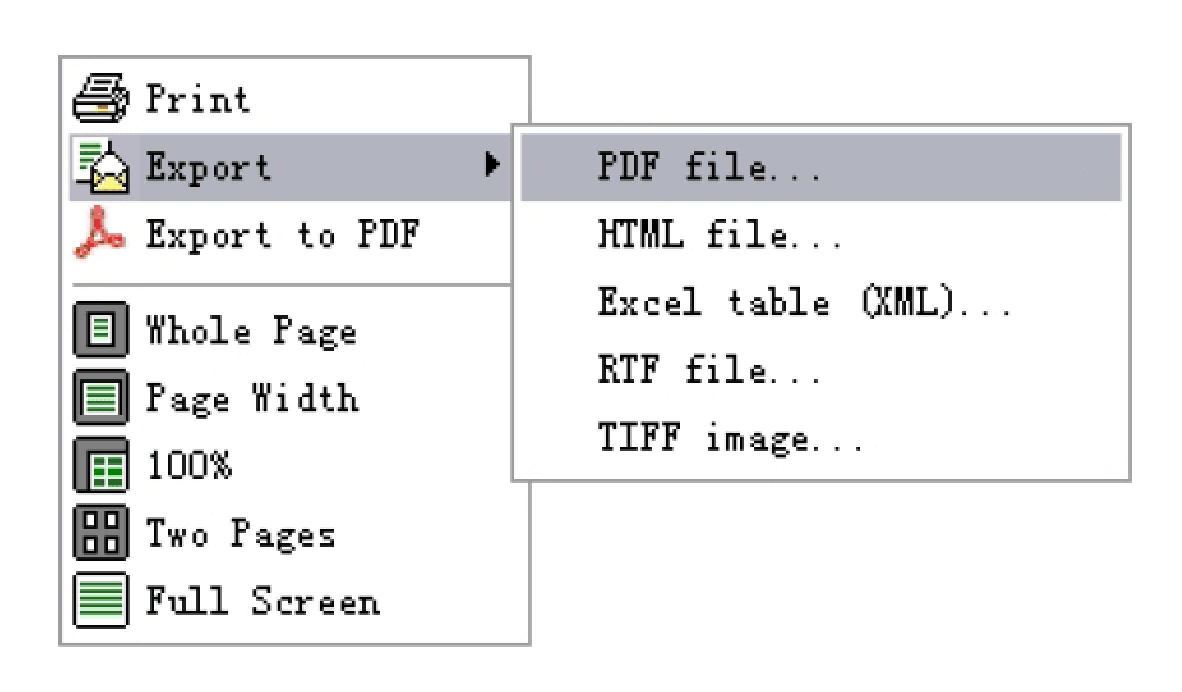


图 10-50　选择报表导出的文件类型

10.2.3　Browser 网页浏览视图

在 Views 导航中选择 Browser 选项，即可进入 PRTG 网页管理模式，如图 10-51 所示。在 PRTG 中进入 Browser 界面与在 Explorer 浏览器中查看 PRTG 显示同样的内容。也

可以在该界面的左上角，在 URL 连接位置打开右键菜单，选择在浏览器中要打开的界面即可，如图 10-52 所示。或者选择主界面中的菜单命令 Views | Open Web View In Browser，同样能在浏览器中打开 PRTG 管理界面。

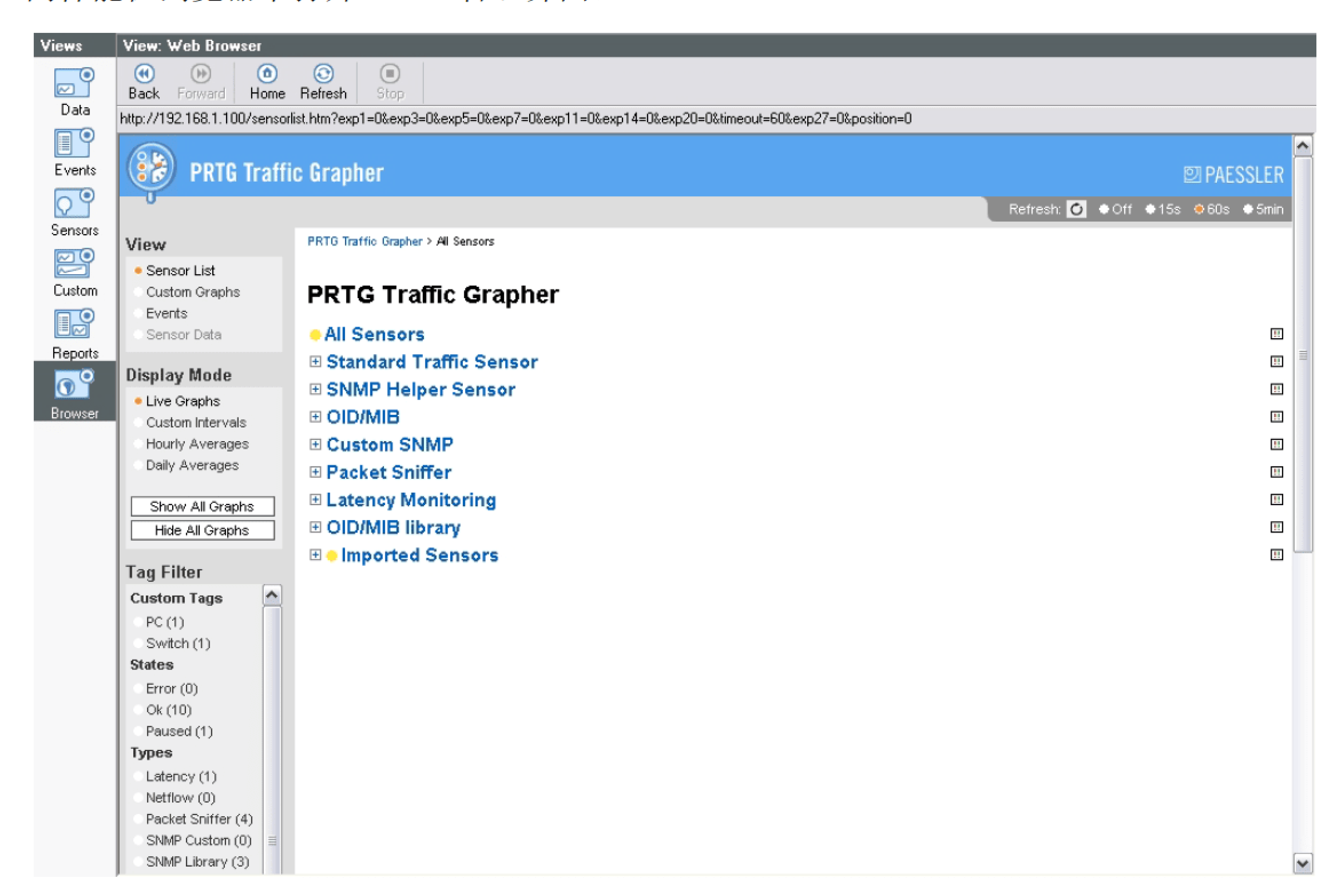


图 10-51 PRTG Browser 管理界面



图 10-52 通过 Browser 界面进入 Explorer 界面

以下分别介绍 Web 模式中的界面功能。

（1）在 Browser 界面的左侧列出了 4 种视图和 4 类显示模式。视图包括 Sensor List（节点列表）、Custom Graphs（用户自定义面板图）、Event（事件）和 Sensor Data（节点数据）。显示模式包括 Live Graphs（实时图像）、Custom Intervals（自定义时段内容）、Hourly Averages（小时平均值）、Daily Averages（每日平均值），如图 10-53 所示。

（2）在主界面的主窗口中列出了所有节点及其监测接口列表，如图 10-54 所示。

单击节点右侧的图标 能够展开对应节点的曲线图（Graphs）、数据表（Data）和事件列表（Event）。

（3）如果需要按照自定义标签、节点类型、节点状态来查看各节点信息，则可通过 Tag Filter 面板来进行节点的过滤查看，其功能与 PRTG 控制台界面功能相似，如图 10-55 所示。

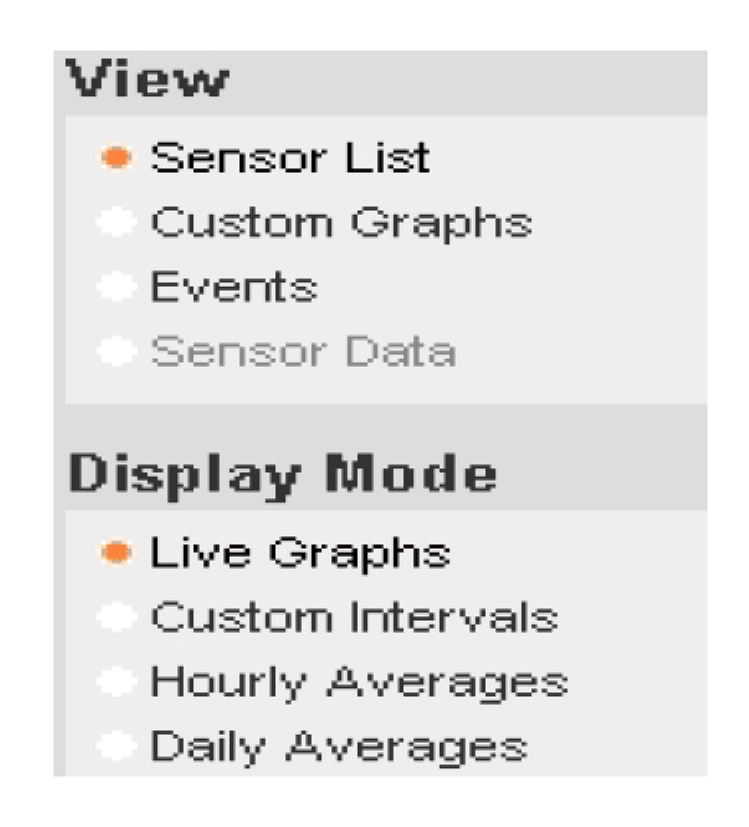


图 10-53　网页模式下的视图和显示模式



图 10-54　节点及监测接口列表

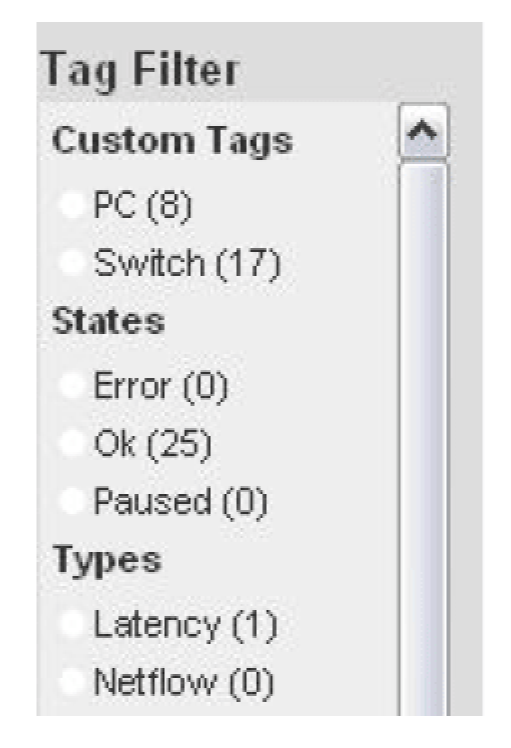


图 10-55　按照 Tag Filter 查看节点信息

10.3　PRTG 中的其他功能项及设置

1．查看历史数据的功能

查看历史数据的功能能够查看指定节点的任意时间段内的图表和数据表。选择主界面

3．PRTG 运行日程设置

运行日程设置定义 PRTG 执行监测和发送提示信息的时间段。选择 PRTG 主界面菜单命令 Extras | Options，选择 Schedules 页面即可新建、重命名或删除日程安排项目，如图 10-58 所示。

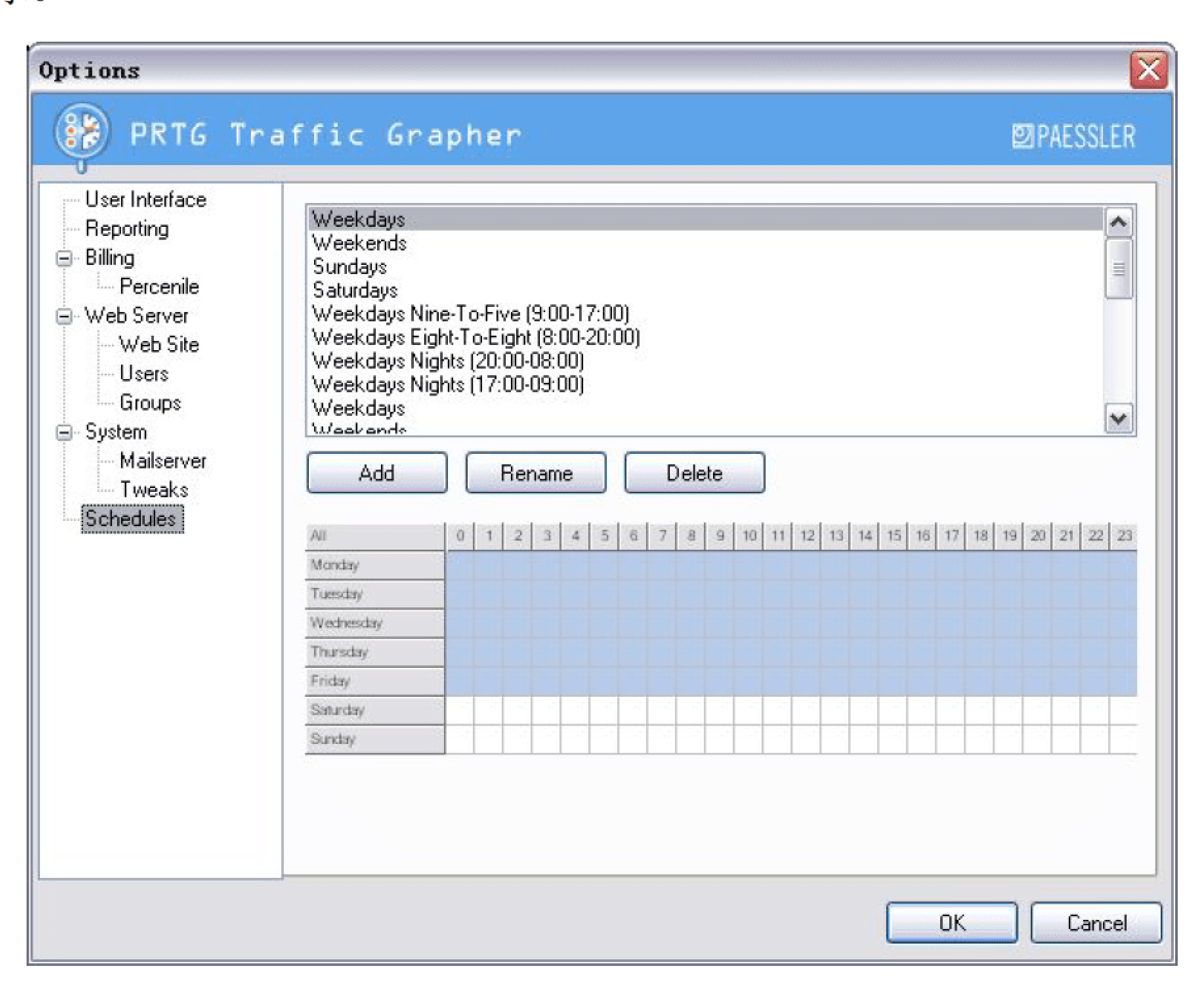


图 10-58　Schedules 设置

在图 10-58 中，日程表纵向列出了周一至周日的选项，横向为 1～24 小时的选项，只要在对应的表格中选择为蓝色方块的就是指定了 PRTG 的运行日程表。默认 PRTG 使用 Weekdays 日程，即在周一至周五的全天 24 小时时段内，执行监测节点和发出提示信息的任务。

10.4　本章小结

通过本章的介绍，读者可以掌握 PRTG 的各项功能、详细设置和报表视图的应用等。针对网络流量监测，网管员需要持续地关注网络中数据流量的变化，以了解发生异常峰值的原因，并针对异常情况做出结构调整和优化。

第 11 章　Kiwi Syslog 安装及设备配置

日志服务器用于收集网络中各种设备的日志信息，并作为网络状态分析、故障解决和网络优化的重要途径，同时它也是对复杂的网络设备实现统一管理的一种方式。搭建日志服务器需要一款具备兼容性、易用性、通用性的日志管理程序。本书推荐目前应用较为广泛的专业日志程序 Kiwi Syslog Deamon。

本章首先介绍 Kiwi Syslog 的主要功能、特征和支持的硬件对象等信息，还介绍了程序安装过程等内容。然后介绍目前较为通用的 Syslog 日志系统，内容包括 Syslog 数据格式、参数类型、日志级别划分等，还介绍了 Windows 系统、Linux 系统、路由器和交换机设备中的日志管理，以及将日志信息发送至 Kiwi Syslog 服务器的配置方法，以实现各类日志信息的集中管理。

11.1　Kiwi Syslog 程序简介及安装

11.1.1　Kiwi Syslog Deamon 介绍

网络中会生成各类日志信息，例如主机遭到入侵、设备无故重启或关闭、网络设备传输中断、应用程序报错、服务停止运行等等。汇总这些日志信息，就能够查找和分析这些不明原因的故障、了解网络运行异常状况以及作为安全审计的证据。

在庞大的网络中，日志服务器显得尤为重要。默认各类设备均会在本地磁盘记录日志信息。当设备较多的时候，如果需要逐台登录设备查看日志，无疑是件很大的工作量。而且故障发生时，往往需要登录到多台设备中才能查找到真正的原因。另外，在安全方面，一旦主机被入侵，入侵者将会删除所入侵记录，使得系统管理员无法获取任何安全审计信息。将各类设备日志信息集中到一台服务器中进行统一管理，将更方便日志信息的存储、查找和分析。

Kiwi Syslog Deamon 是一个居于 Windows 平台的免费 Syslog 应用程序，它能够接收、记录、显示和转发来自于支持 Syslog 的系统日志消息，例如路由器、交换机、Unix 系统以及其他网络设备，并能够实时展示接收到的日志信息。

Kiwi Syslog 支持的设备有：

- CiscoRouter；
- CiscoPIX；

- Cisco 交换机；
- Unix 主机；
- 3COM dlink 网络设备；
- Netscreen 防火墙、Symantec 防火墙和 VPN；
- FREESCO 路由器和防火墙；
- Intertex ADSL 路由器；
- HP JetDriect printer；
- 支持 SNMP 协议和有 Syslog 选项的设备。

11.1.2 Kiwi Syslog 程序功能

Kiwi Syslog Deamon 是完全免费的版本，可通过其官方网站 www.kiwisyslog.com 进行下载，并获取使用手册。免费版本能够用于 Windows NT/2000/XP 系统。Kiwi Syslog 注册版本可通过其官方网站或授权代理进行购买。注册版本支持更多的 Windows 系统，并包含更多扩展功能。

注册版中除了提供免费版本的功能外，还增加了分类存储日志文件方式、日志信息过滤方式、发送日志方式、缓存容量和 DNS 处理能力等。如果网络结构较为简单，仅作为收集和分析网络日志用，免费的版本已经能够满足使用。

Kiwi Syslog Deamon 应用程序包含以下功能：

- 在滚动换行的 Windows 图形界面窗口中显示日志信息；
- 实时记录接收到的信息到 Text 文本；
- 记录或转发所有日志信息至另一台 Syslog 服务器，或基于优先级、时间段记录和转发日志；
- 可通过 ODBC 将日志记录到数据库；
- 可将日志记录到 NT 操作系统中的应用程序日志中；
- 可将日志信息通过 SMTP 发送到指定 E-mail 邮箱；
- 可通过声音或 E-mail 方式，每小时发送信息报警提示，以及发送 Log 文件过大的报警提示；
- 每天通过 E-mail 方式发送日志统计情况；
- 通过图表方式统计并展示前 24 小时和前 60 分钟的系统日志；
- 调用其他外部应用程序，例如 paging notification system；
- 能够通过 Notepager Pro（短信发送程序）发送短信息至手机；
- Kiwi Syslog Deamon 在接收消息时能够将主机名、主机 IP 地址、优先权、消息内容和时间段进行过滤。

11.1.3 Kiwi Syslog 程序特征

Kiwi Syslog Deamon 应用程序包含以下特征：

以下分别介绍这 3 个数据的组成部分。

1．PRI 部分

PRI 是 Priority（优先权）的缩写，该数值在文本中用“<>”进行标识，取值范围从 0～191，该参数由 Facility 和 Level 共同定义。PRI 项的数值通过如下公式进行计算：

Priority = Facility ∗ 8 + Level

而日志服务器对消息进行解析时公式为：

Facility = Priority / 8； Level = Priority % 8（例如，1=15/8；7=15%8）

Facility 项说明：该参数是 Syslog 中的一个重要参数，用于说明触发日志信息的模块，只要是支持标准 Syslog 服务的操作系统，都遵循同样的 Facility 定义，共包含 24 个子项，Facility 详细类型参数见表 11.1。

表 11.1　Facility 参数类型列表及描述

Facility 类型	功能和描述	符　　号	Syslog 序列号
Kern	内核信息	LOG_KERN	0
user	用户进程	LOG_USER	1
E-mail	电子邮件	LOG_MAIl	2
Daemon	后台进程，与 inetd 守护进程有关的信息	LOG_DAEMON	3
Authpriv	认证和授权信息	LOG_AUTH	4
Syslog	系统日志	LOG_SYSLOG	5
Lpr	打印服务相关信息	LOG_LPR	6
News	新闻服务器日志信息	LOG_NEWS	7
Uucp	Uucp 程序生成的信息	LOG_UUCP	8
Cron	cron 和 at 相关的信息，即计划和任务信息	LOG_CRON	9
Local0～local7	自定义程序使用，如 Local5 为 ssh 使用	LOG_LOCALn	16～23

Level 项说明：该参数用于表示日志信息的重要级别，包括 Emerg、Alert 等共计 9 个类别，其类别见表 11.2。

表 11.2　Level 参数类型及描述

序号	Level 项目	注释（按降序排列，严重性越来越低）
1	emerg	致命错误，系统不可用
2	alert	需要立即采取补救措施
3	crit	阻止某些工具或子系统功能实现的关键错误
4	err	阻止工具或某些子系统部分功能实现的错误
5	warning	警告信息
6	notice	需要注意的信息
7	info	提供通知信息的消息
8	debug	调试信息
9	none	没有优先级，通常用于排错

如果需要保存日志信息，可以将事件日志存档为 3 种格式：日志文件格式.evt、文本文件格式.txt、逗号分隔的文本文件格式.csv。

在【事件查看器】中，在要存档的日志信息类别中打开右键菜单，并选择【另存日志文件】命令，然后选择文件保存位置和保存类型即可，如图 11-8 所示。



图 11-7 通过事件查看器查看 Windows 日志

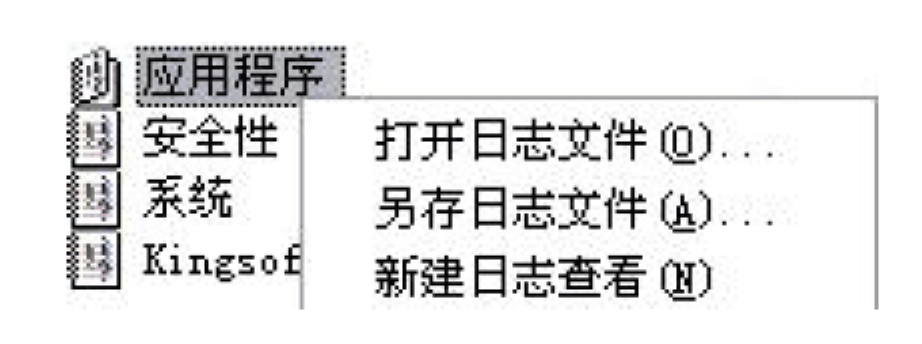


图 11-8 保存日志信息

以下分别介绍 3 类 Windows 日志信息。

1．系统日志信息

系统日志信息记录系统进程和设备驱动程序的活动。包括启动失败的设备驱动程序、硬件错误、重复的 IP 地址，以及服务进程的启动、暂停和停止。例如，Windows 系统启动期间要加载的驱动程序失败，或者其他系统组件出现故障。

例如，在【控制面板】|【服务】中将 SNMP 服务 SNMP Service 项目停止，那么停止 SNMP 的日志信息将记录在系统类日志中。打开【事件查看器】，即可查看关于 SNMP Service 服务的停止日志信息，如图 11-9 所示。



图 11-9 Windows 日志信息查看

在图 11-9 中列出了信息产生的日期、时间、描述、事件 ID 和信息来源等。此处特别说明一下事件 ID 和来源。Windows 的日志信息并不是 Windows 自身产生的，而是由各个独立的应用程序或组件生成。ID 和来源则标识了日志信息的程序或组件。通过 ID 和来源，可在官方网站 www.eventid.net 中查询到更为详细的解释。

例如，查询 ID 为 17，事件来源为 W32Time 的解释，可看到该网站提供的关于该日志信息的两种解释，可能由于存在多个时间提供源且无法获取时间，导致终端无法得到确切的时间源，或由于时间提供程序 NtpClient 报错而导致错误信息的产生，如图 11-10 所示。

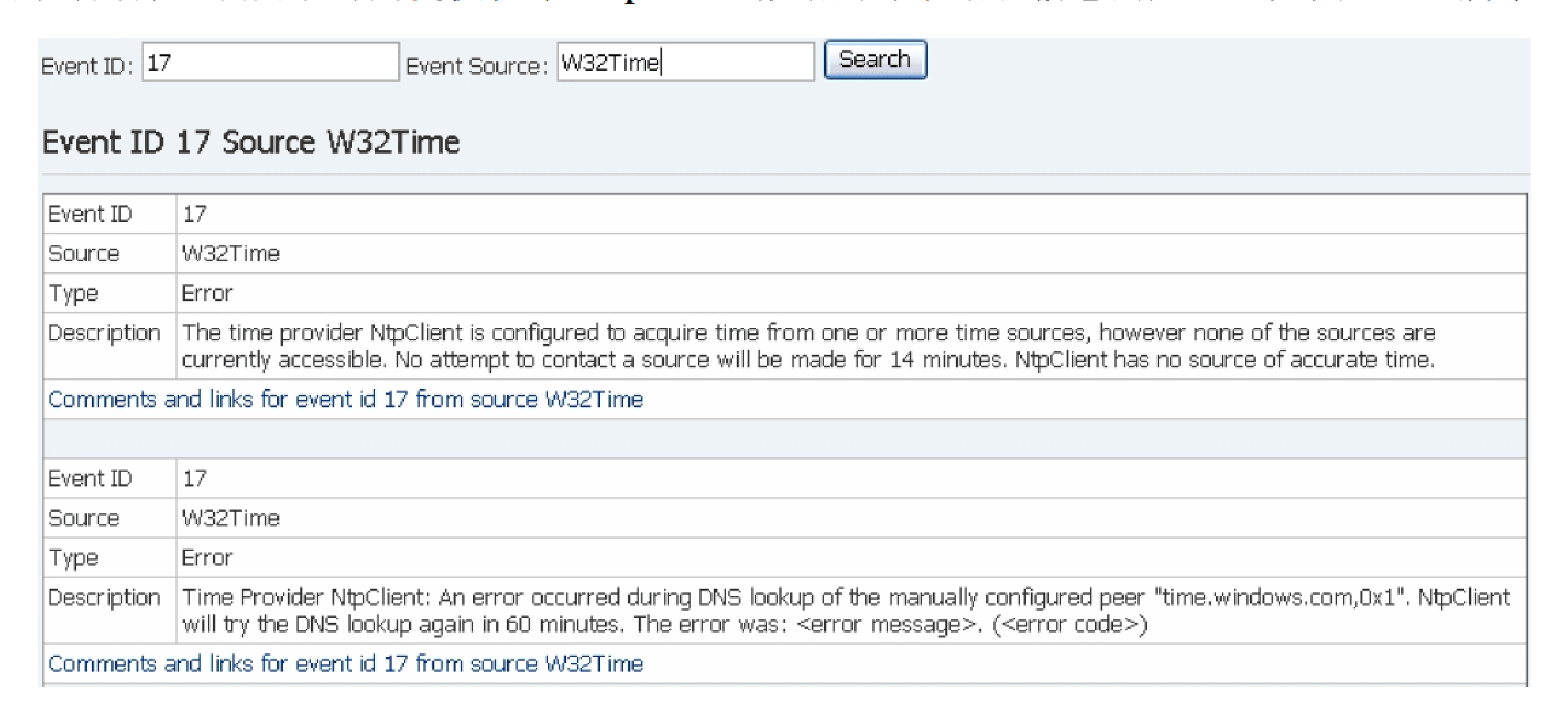


图 11-10　通过 eventid.net 获取更多的日志信息解释

2. 应用程序日志

应用程序日志包括应用程序运行方面的日志信息。它记录的应用程序事件包括所有程序错误、程序启动停止及程序运行产生的信息。例如，程序失败登录的次数、磁盘使用的情况、文件错误和其他程序故障。

3. 安全日志

安全日志通常是在应急响应处理阶段最有用的日志。它主要用于审计和管理用户登录及权限等方面的信息。它审核的安全事件包括用户权限的变化、文件和目录访问、打印、系统登录和注销及与资源使用有关的信息，例如创建、打开或删除应用文件。

管理员可以指定在安全日志中记录的事件。例如启用了登录审核，那么系统登录尝试就记录在安全日志中，在安全设置中开启对用户登录审核的操作步骤如下：

（1）在【控制面板】|【管理工具】中选择【本地安全设置】，其中包含了系统对各项操作的审计，默认均为不审核，如图 11-11 所示。

（2）选择【审核登录事件】选项，并选择对“成功”和“失败”的操作审计，则用户成功登录或登录失败的日志均会记录到安全日志中，如图 11-12 所示。

的识别。本书中仍介绍目前主流的 Syslog 机制。

1. Linux 系统日志组成

- 日志文件：存储日志信息的文件位于/dev/log 目录，用于接收并记录系统和程序产生的日志信息。
- 守护进程：该进程为/sbin/syslogd，在系统初始化时自动启动，监控系统和程序产生的日志信息，并将信息记入日志文件中。
- 配置文件：主要配置文件的默认位置是/etc/syslog.conf，为守护进程提供配置信息，用于指定日志记录规则。

2. Linux 系统日志分类

按照日志内容的类别划分，可分为如下 3 类。

- 连接时间日志：由多个程序执行，把记录写入到/var/og/wtmp 和/var/run/utmp 文件中，并不断更新 wtmp 和 utmp 文件，使系统管理员能够跟踪谁在何时登录到系统。
- 进程统计日志：由系统内核执行，当一个进程终止时，为每个进程写一个记录至统计文件（pacct 或 acct）中。进程统计是对系统中基本服务的使用情况进行统计。
- 错误日志：各种系统守护进程、用户程序和内核将错误信息记录到文件/var/og/messages 中。记录需要注意或异常状态的事件。

3. 常见的日志文件

Linux 系统中，如果未对配置文件/etc/syslog.conf 进行过特别的配制，日志默认存储位置是/var/log 目录。进入该目录可看到各类日志文件，常见的日志文件见表 11.3。

表 11.3 Linux 系统中常见的日志文件

序号	日志文件名	描　述
1	access-log	记录 HTTP/Web 的传输
2	acct/pacct	记录用户命令
3	aculog	记录 MODEM 的活动
4	btmp	记录失败的纪录
5	lastlog	记录最近几次成功登录的事件和最后一次不成功的登录
6	Messages	从 Syslog 中记录信息，包括系统和程序错误信息或异常状态等日志
7	sudolog	记录使用 Sudo 发出的命令，包括用户执行命令或操作的行为记录
8	sulog	记录用户使用 su 命令的记录
9	syslog	从 Syslog 中记录信息，通常只记录警告信息
10	utmp	该日志文件记录有关当前登录的每个用户的信息
11	wtmp	该日志文件永久记录每个用户登录、注销及系统的启动、停机的事件
12	xferlog	记录 FTP 会话，显示用户上传至 FTP 服务器或从 FTP 服务器下载的文件
13	maillog	每一个发送到系统或从系统发出的电子邮件

11.4.2 查看 Linux 日志命令

more 命令：常用的 Linux 查看文件命令，通常用于查看超过一屏幕的文件。执行该命令的结果如图 11-18 所示。

```
[root@RedhatServerlog]#more messages
Mar 21 12:26:50 RedhatServer syslogd 1.4.1: restart.
Mar 21 12:30:08 RedhatServer su(pam_unix)[2629]: session opened for user news
 (uid=0)
Mar 21 12:30:08 RedhatServer su(pam_unix)[2629]: session closed for user news
Apr 11 16:31:56 RedhatServer syslogd 1.4.1: restart.
Apr 11 16:31:56 RedhatServer syslog: syslogd startup succeeded
Apr 11 16:31:56 RedhatServer kernel: klogd 1.4.1, log source = /proc/kmsg star
d.
Apr 11 16:31:56 RedhatServer kernel: Linux version 2.4.20-8 (bhcompile@porky.d
el.redhat.com) (gcc version 3.2.2 20030222 (Red Hat Linux 3.2.2-5)) #1 Thu Mar
3 17:54:28 EST 2003
Apr 11 16:31:56 RedhatServer kernel: BIOS-provided physical RAM map:
Apr 11 16:31:56 RedhatServer kernel:  BIOS-e820: 0000000000000000 - 0000000000
f800 (usable)
Apr 11 16:31:56 RedhatServer kernel:  BIOS-e820: 000000000009f800 - 0000000000
```

图 11-18 More 命令

who 命令：查询 wtmp 和 utmp 文件。这两个文件都是二进制文件，需要使用专门的命令进行查看。who 命令查询 utmp 文件并报告当前登录的每个用户。该命令的默认输出包括用户名、终端类型、登录日期及远程主机。执行该命令的结果如图 11-19 所示。

```
[root@RedhatServerlog]#who
root      tty1          Apr 11 21:23
root      :0            Apr 11 21:16
```

图 11-19 Who 命令

w 命令：查询 utmp 文件，显示当前系统中的用户及该用户所运行的进程信息。执行该命令的结果如图 11-20 所示。

```
[root@RedhatServerlog]#w
 21:26:21  up 11 min,  2 users,  load average: 0.00, 0.04, 0.05
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU  WHAT
root     tty1     -                 9:23pm  0.00s  0.07s  0.01s  w
root     :0       -                 9:16pm   ?     0.00s  0.39s  /usr/bin/gnome
```

图 11-20 W 命令

users 命令：用单独的一行打印出当前登录的用户，每个显示的用户名对应一个登录会话。如果一个用户有不止一个登录会话，那么该用户名将显示相同的次数。执行该命令的结果如图 11-21 所示，

```
[root@RedhatServerlog]#users
root root
```

图 11-21 Users 命令

last 命令：往回搜索 wtmp 来显示自从文件第一次创建以来登录过的用户记录，如图 11-22 所示。

别而不包括大于它的优先级；如果在“=”前加上“!”，则表示求反；如果使用“*”则表示使用任何优先级别，即和使用 Debug 级别的结果是一样的。例如：

```
mail.*;mail.!info/var/log/mail
```

该语句中，mail.*将发送所有的消息，但 mail.!info 却把 info 优先级的消息排除在外，意思是将除 info 优先级以外的所有消息发送到/var/log/mail 文件中。

11.4.4 配置文件的内容解释

在了解了配置规则和特殊符号意义后，可通过 More 命令来查看配置文件的内容。下面将对配置文件 syslog.conf 中的内容进行注解，以帮助网管员更好地理解配置规则。

Syslog.conf 配置文件的内容和注解如下：

```
[root@RedhatServer root]# more /etc/syslog.conf
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.* /dev/console
# Log anything （except mail） of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages
//将 info 或更高级别的消息送到/var/log/messages，除 mail 外

# The authpriv file has restricted access.
authpriv.* /var/log/secure，
//安全验证日志，将 authpirv 设备的任何级别信息记录到/var/log/secure 文件中

# Log all the mail messages in one place.
mail.* /var/log/maillog
//电子邮件系统日志，将 mail 设备中的任何级别的信息记录到/var/log/maillog 文件中

# Log cron stuff
cron.* /var/log/cron  //计时信息，将 cron 设备中任何级别的信息记录到/var/log/cron
                        文件中

# Everybody gets emergency messages
*.emerg *
//emerg 级别的日志表示系统已经不可用，将任何设备的 emerg 级别的信息发送给所有正在系统
  上的用户
```

```
# Save news errors of level crit and higher in a special file.
Uucp,news.crit /var/log/spooler
//crit 表示危急级别的日志信息，将 uucp 和 news 设备的 crit 级别的信息记录到
/var/log/spooler

# Save boot messages also to boot.log
local7.* /var/log/boot.log
//开机系统日志，用 local7 来表示，将和系统启动相关的信息记录到/var/log/boot.log 文
  件中
```

11.4.5 配置 Linux 发送日志至远程服务器

在修改配置文件内容之前，建议首先将 Syslog.conf 文件进行备份，以防止配置错误而造成文件的损坏。备份命令如下：

```
[root@RedhatServeretc]#cp /etc/syslog.conf /etc/syslog.confBAK
```

如果需要还原文件，同样使用该命令，用备份文件替换更改的配置文件即可。命令如下：

```
[root@RedhatServeretc]#cp /etc/syslog.confBAK /etc/syslog.conf
```

配置 Linux 发送日志至远程服务器，命令格式如下：

```
facility.level @address
```

其中，参数@表示发送远程记录，将日志信息发送到远程日志服务器；address 参数可以是 IP 地址或域名。

实例 1：#将所有级别的内核日志发送到远程 Syslog 服务器，IP 为 172.16.6.168。

```
kern.* @172.16.6.168
```

#将 warning 以上的所有类别日志信息发送至远程服务器，命令如下：

```
.* warning @172.16.6.168
```

实例 2：# 将所有级别的内核日志发送到终端。

```
kern.* /dev/console
```

#将所有类型的所有级别的日志记录到/var/log/messages 文件。

```
*.* /var/log/messages
```

#将所有 info 级别以上的信息，不包括 mail 类型所有级别和 authpriv 类型的 err 级别信息，记录到/var/log/messages 文件。

```
*.info;mail.none;authpriv.!err        -/var/log/messages
```

```
[H3C-S3600]info-center source default channel loghost debug state off
[H3C-S3600]info-center source default channel loghost log state off
[H3C-S3600]info-center source default channel loghost trap state off
```

将 IP 地址为 172.168.6.168 的主机作为日志主机，设置生成日志信息的子系统名称为 Local7，命令如下：

```
[H3C-S3600]info-center loghost 172.16.6.168 facility local7
```

设置输出日志信息级别为 informational，允许输出信息的模块为所有模块，命令如下：

```
[H3C-S3600]info-center source default channel loghost log level informational
```

11.6 本章小结

本章中介绍了 Linux Syslog 系统机制。特别需要关注 Syslog 日志的分类和级别划分。只有明确了日志的来源和重要级别，才能读懂 Linux 日志信息的含义。本章还介绍了配置 Windows 和 Linux 系统以及路由器、交换机日志发送到指定服务器的方法。不同厂商和型号的网络设备配置方式会有所差异，网络管理员可根据实际情况查阅相关技术文档。

第 12 章　Kiwi Syslog 功能与程序配置

本章主要介绍 Kiwi Syslog 程序的各项功能及设置，包括如何使用 Kiwi 接收和过滤日志信息、将日志信息存储到数据库中、发送 E-mail 报警提示信息等，以及当 Kiwi 程序无法正常接收信息的检查和处理方法。内容如下：

- ❑ 程序主界面和菜单介绍；
- ❑ 程序各设置项介绍；
- ❑ 程序运行故障检查和排除。

通过本章的学习，能够详细了解 Kiwi 程序的功能，从而更好地使用该程序。

12.1　程序主界面及菜单介绍

12.1.1　程序主界面

Kiwi Syslog 主界面中包含了主菜单项、快捷按钮、日志显示窗口及程序使用情况的提示信息，如图 12-1 所示。

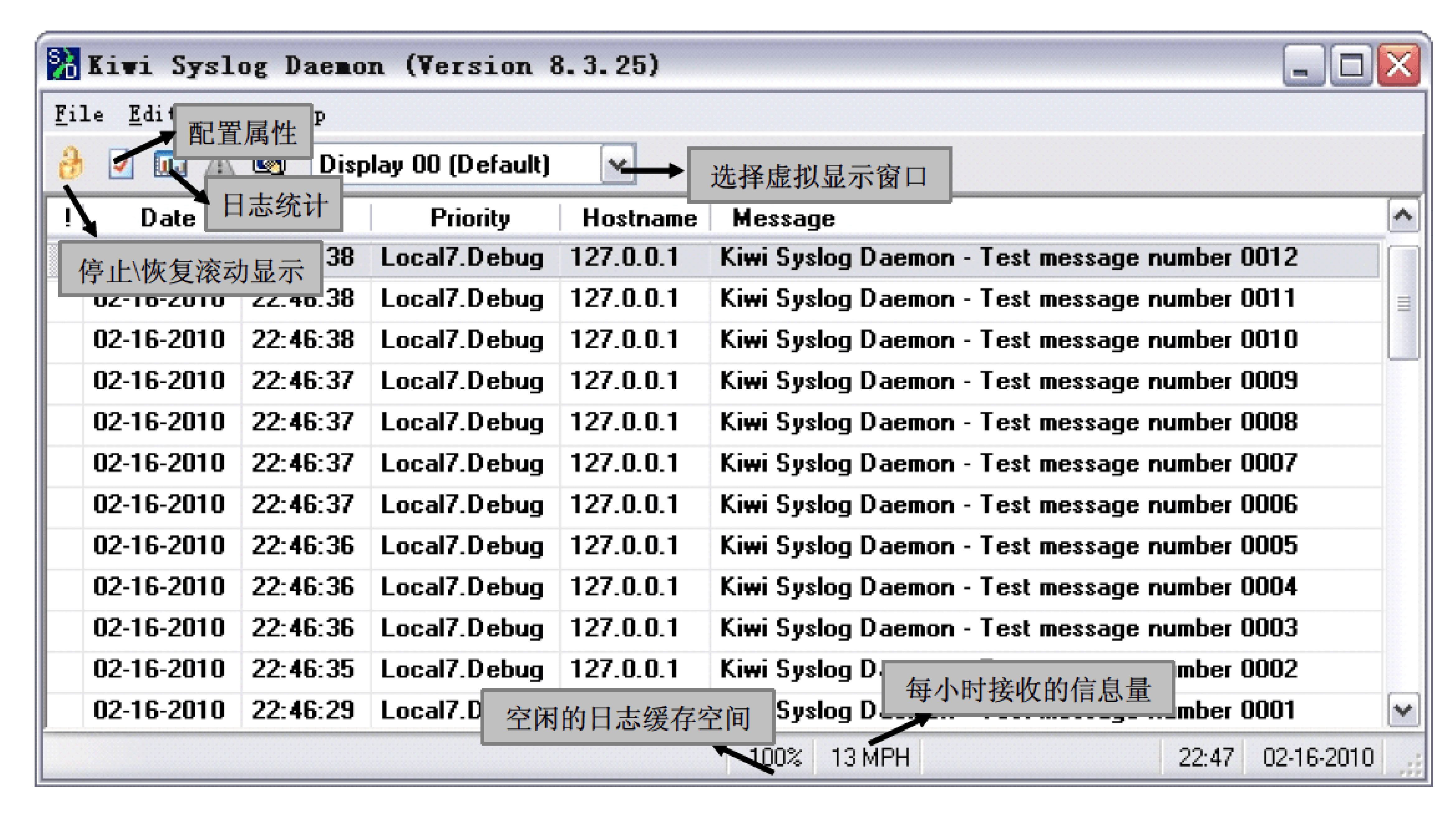


图 12-1　Kiwi 程序主界面

Kiwi 主界面快捷键功能从左至右的功能见表 12.1。

表 12.1 主界面快捷键功能

序号	图 标	介 绍
1		停止/恢复滚动显示
2		打开配置属性窗口
3		显示日志统计图表
4		程序报警提示
5		清除当前界面所有列表信息
6	Display 00 (Default)	选择虚拟显示窗口

12.1.2 File 主菜单命令

在主界面 File 菜单中包括了 Kiwi Syslog 主要功能的配置、测试、数据输入/输出等命令，如图 12-2 所示。以下分别对菜单命令做介绍。

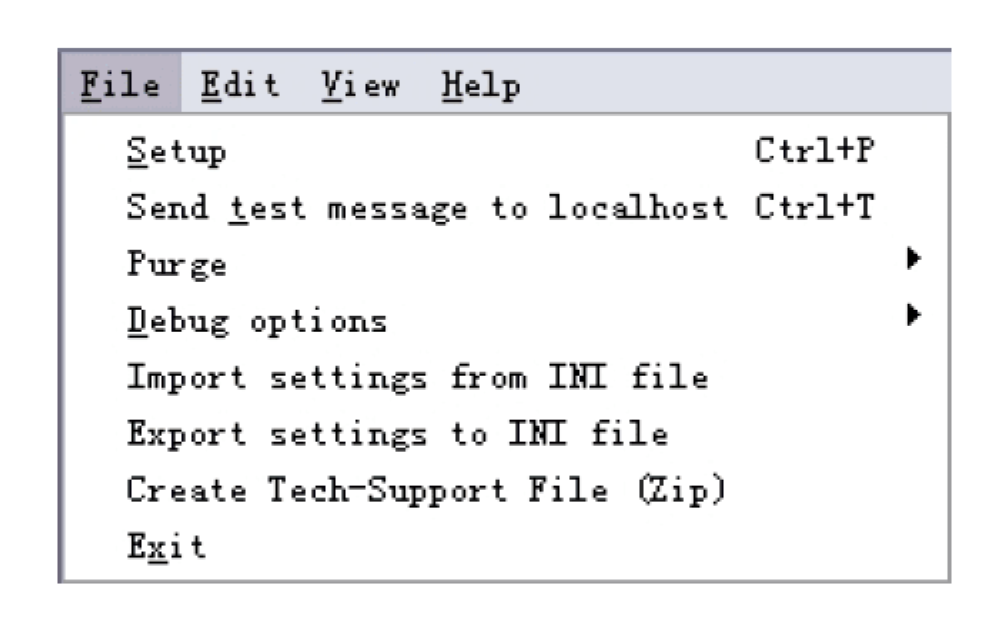


图 12-2 File 菜单

Setup（配置）：选择该菜单命令，可打开 Kiwi Syslog 程序的各项配置，包括过滤规则、数据格式、报警设置等。其详细设置将在后面的使用过程中进行讲解。

Send test message to localhost（发送测试信息）：选择该菜单命令，将通过 UDP 端口发送一条测试信息至本地主机（127.0.0.1），该端口同时也是 Kiwi Syslog 监听的端口，以测试程序功能是否正常运行。

测试信息的格式为：Kiwi Syslog Daemon - Test message number 0001。如需测试程序对 TCP 端口的监听是否正常，可使用该公司的免费测试工具 Kiwi SyslogGen。使用该测试工具同时能够了解 Syslog 日志机制，后面简单介绍该工具的使用方法。如图 12-3 所示为该工具的图标。



图 12-3 Kiwi SyslogGen 测试工具

Purge（清除选项）：可根据需要对日志信息进行清除，包括清除对应的 Text 日志文件，

如图 12-4 所示。

```
Purge e-mail log file
Purge error log file
Purge message queue
Purge mail queue
Purge failed MIB lookup file
Purge database cache
```

图 12-4　清除日志信息菜单命令

其子菜单命令目包括清除 E-mail 日志(对应 SendMailLog.txt)、错误日志(Errorlog.txt)、消息队列（队列缓存数量最多为 1000)、邮件发送队列（缓存数量最高为 1000)、失败的 MIB 查找文件（MIBs\UnknownOIDs.txt)、数据库缓存信息。

Debug Options（调试)：该菜单包括的子菜单命令功能介绍见表 12.2。

表 12.2　Debug Options 菜单命令功能列表

序号	菜 单 命 令	描　述
1	Enable Syslog debug	将所有接收到的原始日志信息记录到 Text 文件中，文件为程序安装目录下的 Syslogd-debug.txt
2	Reset Syslog socket	重置监听端口，清除数据并重新开启对端口的监听
3	Reset all Counters、Timers and Flags	重置所有的计数器、计时器和标志位
4	View message buffer	查看信息缓冲的 Text 文本内容，文件为程序安装目录下的 SyslogMessageBuffer.txt
5	View mail buffer	查看邮件发送队列的 Text 文本内容，文件为程序安装目录下的 SyslogMessageBuffer.txt
6	Clear the Scripe file cache	清除 Scritpe 文件执行的缓存
7	Initialize Custom Statistics	初始化用户自定义的统计信息
8	Clear the Syslog Statistics	清空当前的统计信息
9	View diagnostic information	查看所有诊断信息的 Text 文件，其中包括统计信息、队列缓存信息等

选择 Enable Syslog debug，打开对应的 Syslogd-debug.txt 文件，可看到其中包括了发送时间、源 IP 地址、目的 IP 地址、端口、日志 ID 等信息，如图 12-5 所示。

选择 View message buffer，打开对应的 SyslogMessageBuffer.txt 文件，可看到消息队列的缓存情况等信息。选择 View mail buffer 同样会打开该文件，可查看邮件发送的缓存情况。文件内容如图 12-6 所示。

Create Tech-Support File 菜单命令：选择该命令可在安装目录下生成一个压缩包，其中包括了 INI 配置文件、错误日志文件、Debug 文件、日志诊断文件等一系列 Text 文本文件，作为存档。压缩包内容如图 12-8 所示。

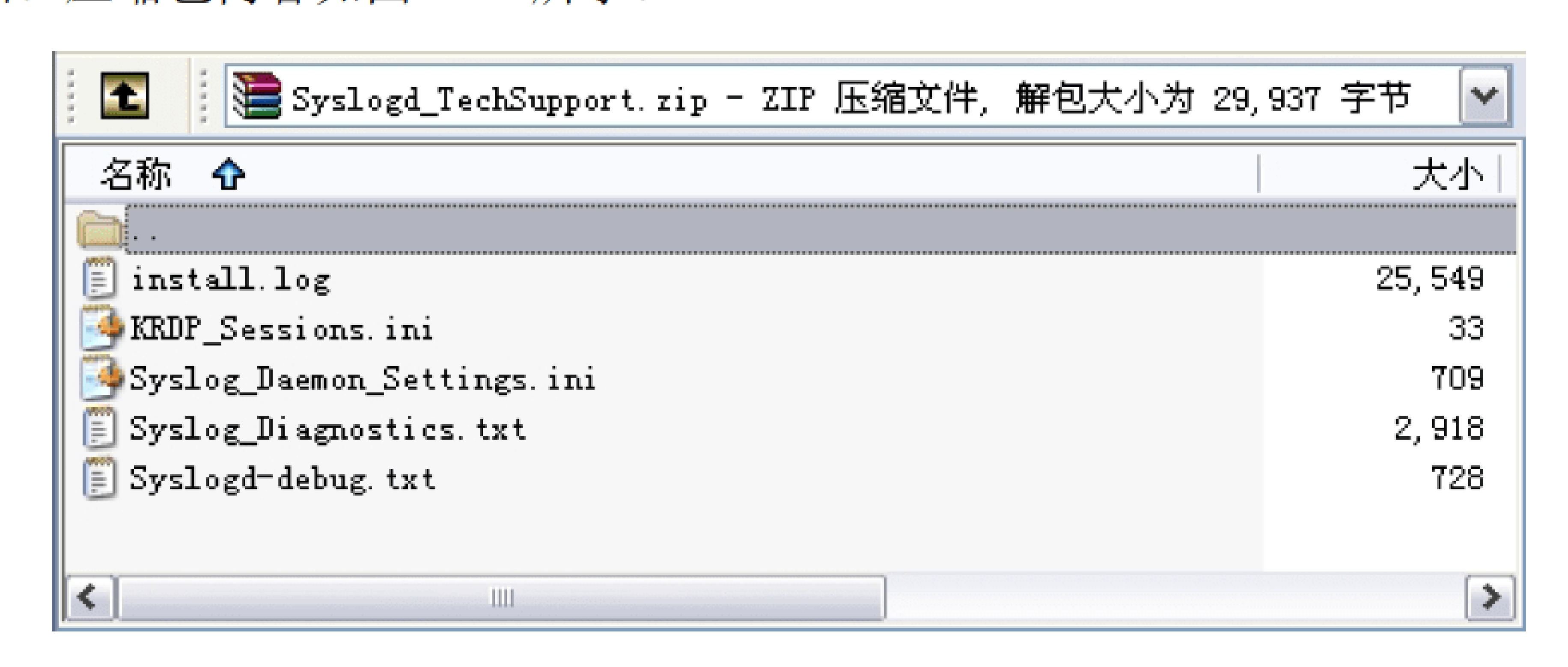


图 12-8　生成相关文件的压缩包

12.1.3　View 主菜单命令

Edit 菜单命令较为简单，仅包括复制信息目录的操作，此处省略。下面介绍 View 菜单命令的内容。打开该主菜单命令，如图 12-9 所示。

View　Help

View Syslog Statistics　Ctrl+S
View e-mail log file　Ctrl+M
View error log file　Ctrl+R
Adjust width to fit screen　Ctrl+W
Highlighting options　Ctrl+H
Clear display　Ctrl+L
Choose font　Ctrl+F
Show/Hide Columns

图 12-9　View 菜单命令

该菜单命令中包括日志统计信息查看、E-mail 日志文件查看、错误日志文件查看、调整程序窗口适应屏幕大小、高亮色彩显示日志信息（该功能注册版本才提供）、清空当前显示界面所有信息、显示字体设置、显示/隐藏显示列。以下介绍统计和高亮显示两项功能。

1. View Syslog Statistics 菜单命令

选择该菜单命令或单击主界面的快捷键按钮可打开统计信息界面，如 12-10 所示。

该日志统计信息每 10 秒钟会更新一次图表。单击 Refresh 按钮或按 F5 键可立即刷新数据并重新计算生成的实时图表。该统计界面包括的图表介绍如下。

- 1 Hour History：该统计图表显示前一个小时内的接收日志数量情况，横轴为时间，

纵轴为每分钟内收到的日志数量合计。该图表从右向左滚动，最左边为前 1 分钟的统计信息，而最右侧为前 1 小时的统计数。

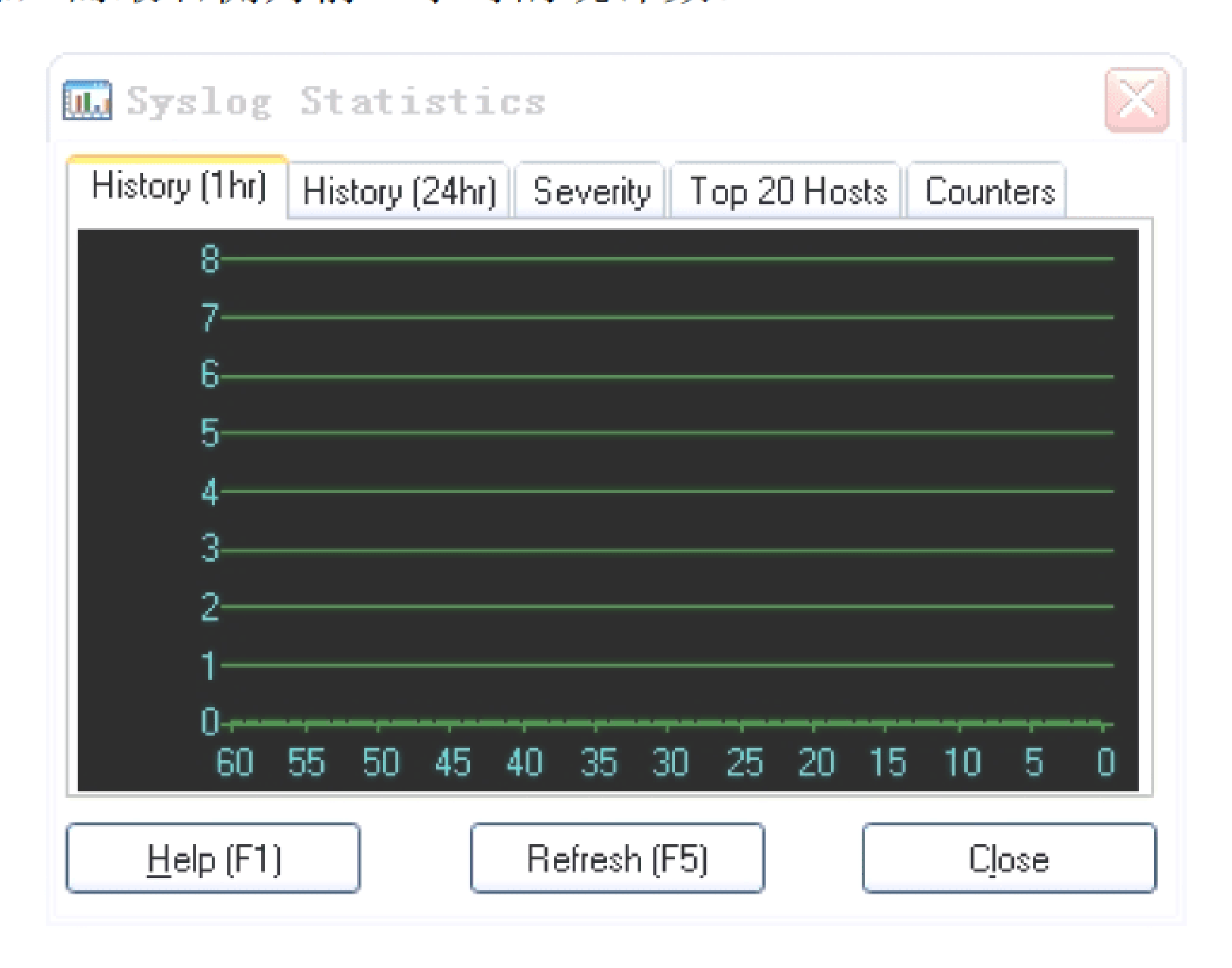


图 12-10　统计窗口界面

- 24 Hour history：展示前了 24 小时内的数量统计情况，纵轴线对应展示每小时内接收的日志数量合计。
- Severity：该页面按故障信息的严重级别进行百分比统计，统计的对象为日志显示界面中所包含的所有日志信息。
- Top 20 Hosts：该页面统计主机产生的日志信息占所有接收信息的百分比，并显示排名前 20 的统计信息。
- Counters：该页面包含一些流量统计及错误信息的统计项，见表 12.3。

表 12.3　统计功能界面的 counters 页面统计项

序号	统 计 项 目	描　述
1	Messages – Total	自程序启动开始接收的日志数量合计
2	Messages - Last hour	前一完整小时内接收的日志数量合计
3	Messages - This hour	从当前开始前 60 分钟内接收的日志数量
4	Messages - Last 24 hours	前 24 小时接收的日志数量
5	Messages - Average	上一小时接收的日志在前 24 小时接收数量中所占百分比
6	Messages - Forwarded:	转发的日志数量
7	Messages - logged to disk:	存储到磁盘的日志数量
8	Errors - logged to disk	程序本身报错且记录到磁盘中的数量
9	Disk space remaining	检测磁盘空间的剩余量，默认设置为 C 盘，用设置界面中的 Alarms|Disk 命令进行设置更改
10	CustomStats1~16	该字段的数据可通过执行脚本获取参数结果传递给该字段进行显示

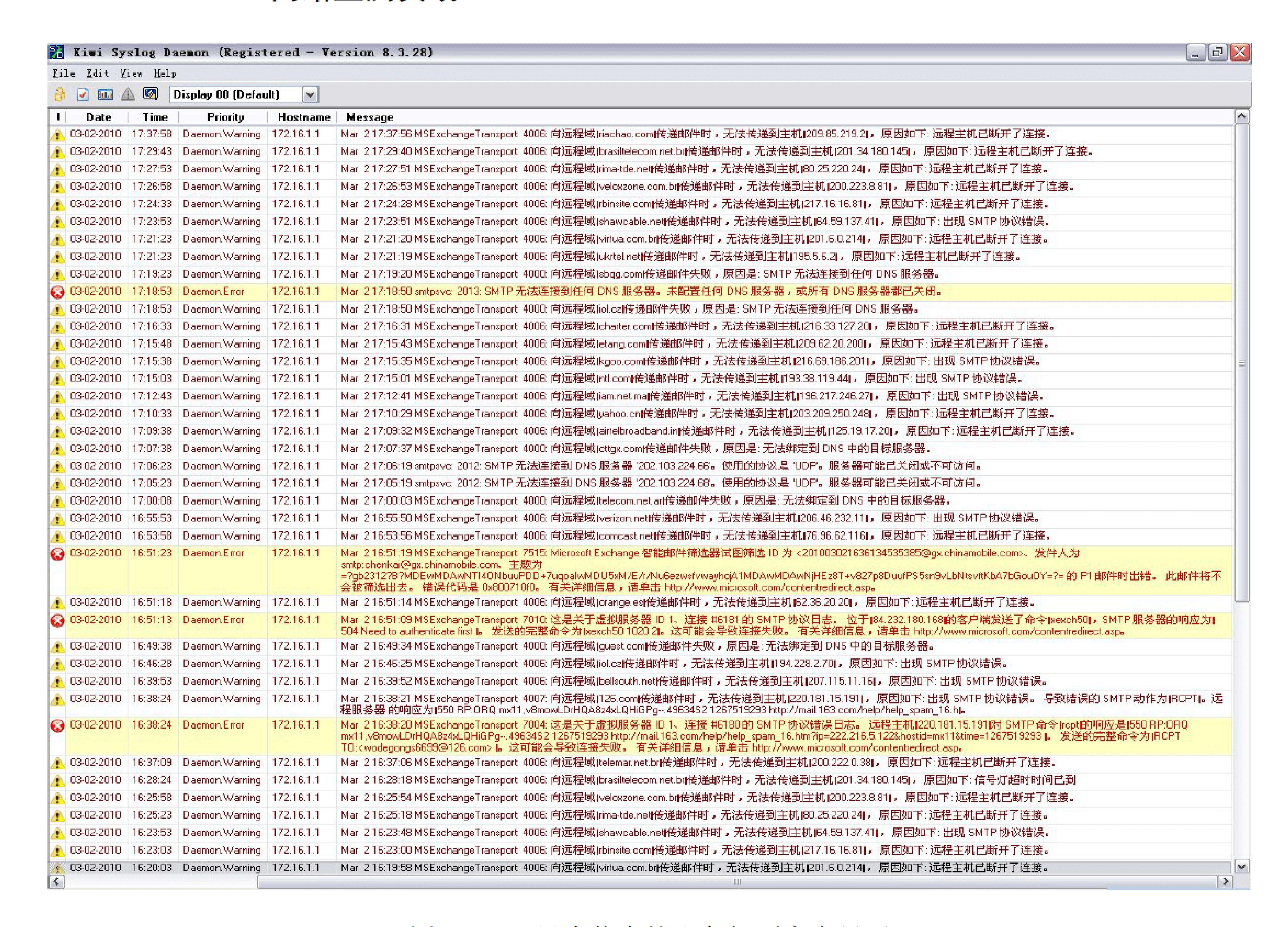


图 12-12 日志信息按配色规则高亮显示

```
Select All
Copy Selected Items
Copy Selected Items as HTML
Highlighting Options
Show/Hide Columns ▶
Choose Font
```

图 12-13 右键菜单



图 12-14 日志显示列

显示列分别为 Icon（图标，注册版本提供）、Date、Time、Priority（优先权）、Hostname、Message（日志内容）。

12.2 属性设置——过滤规则

在对程序界面及菜单命令功能有了初步了解后，即能开始 Kiwi Syslog 的应用了。如果仅作为日志的收集和查看，这些默认的设置项已经能够满足需求。但如果需要更深入地掌握和根据实际需求开展应用，还需了解其更多属性。

下面介绍 Kiwi 的各项功能设置，包括对无用日志信息的过滤、日志的存储、报警动

其执行规则的流程图如图 12-16 所示。

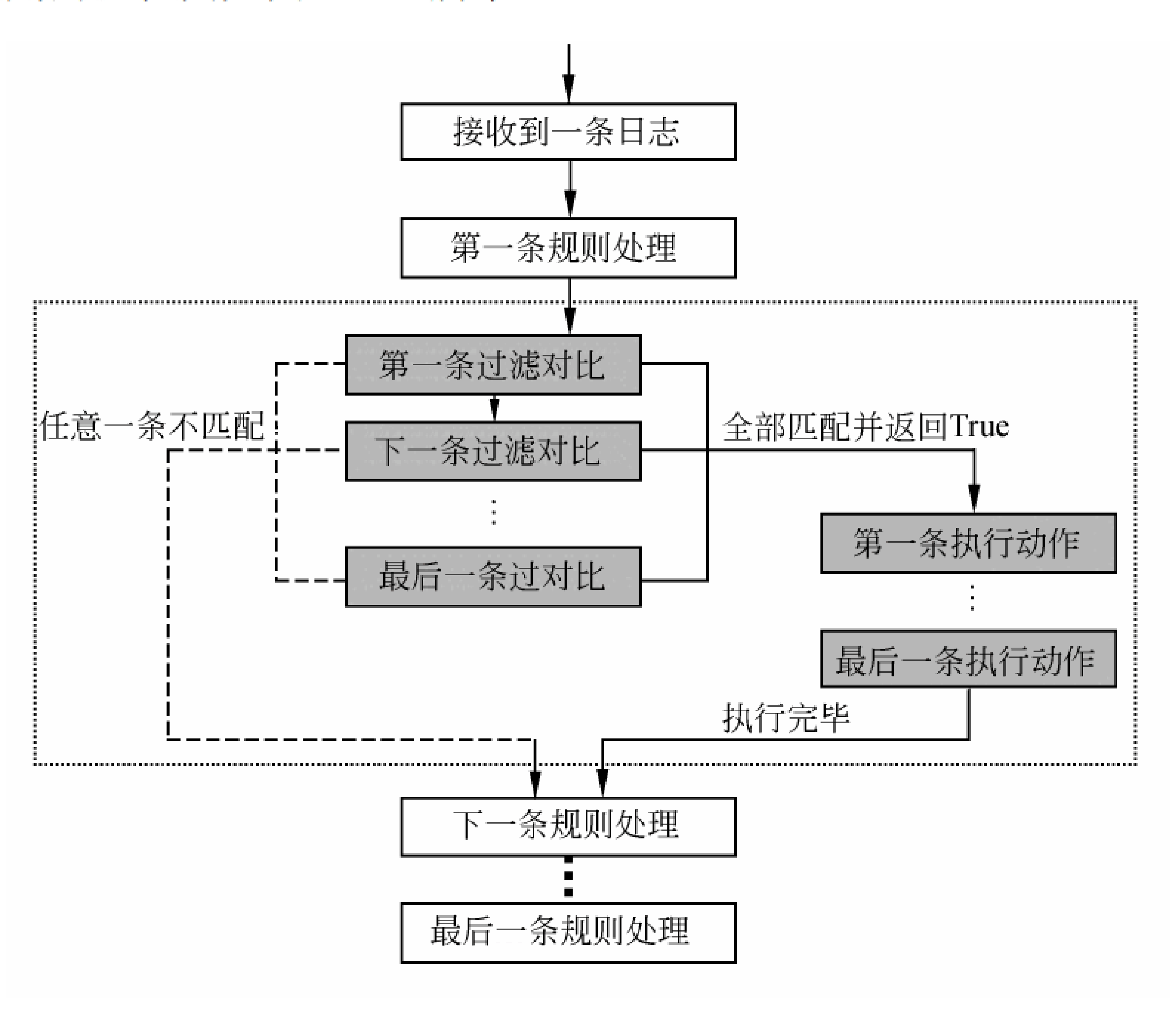


图 12-16　规则执行流程

默认初始安装 Kiwi 程序时仅包含一条命名为 Default 的规则，其中没有包含过滤条件，所有的日志信息都能够通过；但默认规则中包含两条执行动作，分别是显示日志信息和保存信息到文件。默认规则下，所有信息均能够通过界面显示并保存至程序安装目录中\Logs 文件夹下 SyslogCatchAll.txt 文件中。

注意：Kiwi 中允许定义多达 100 条规则，每个规则中可包含多达 100 条过滤规则和 100 个执行动作。

12.2.2　优先级别过滤方式

每一条日志信息都包含一个 Priority（优先级）属性，由 Facility 和 Level 参数构成。使用该过滤方式，选择的优先级与日志信息的优先级进行对比，允许接受与所选优先权匹配的日志信息。该方式能够有效地过滤掉不需要的信息，例如用于登录域、注销域等操作生成的大量 Notice 类别日志信息。

建立优先级过滤步骤如下：

（1）在设置界面左侧列表，选择 Filter 选项，然后单击快捷按钮中的按钮，新建一条过滤条件。

（2）在界面右侧的设置区域的 Field 下拉列表中选择 Priority 选项，在 Filter Type 下拉列表中选择 Priority 方式，如图 12-17 所示。

在图 12-17 中，可按照子系统和信息级别，双击空白表格或在右键菜单中选择 Toggle to ON 命令，对应表格将显示绿色图标，应用并保存后，即完成优先权属性的设置。

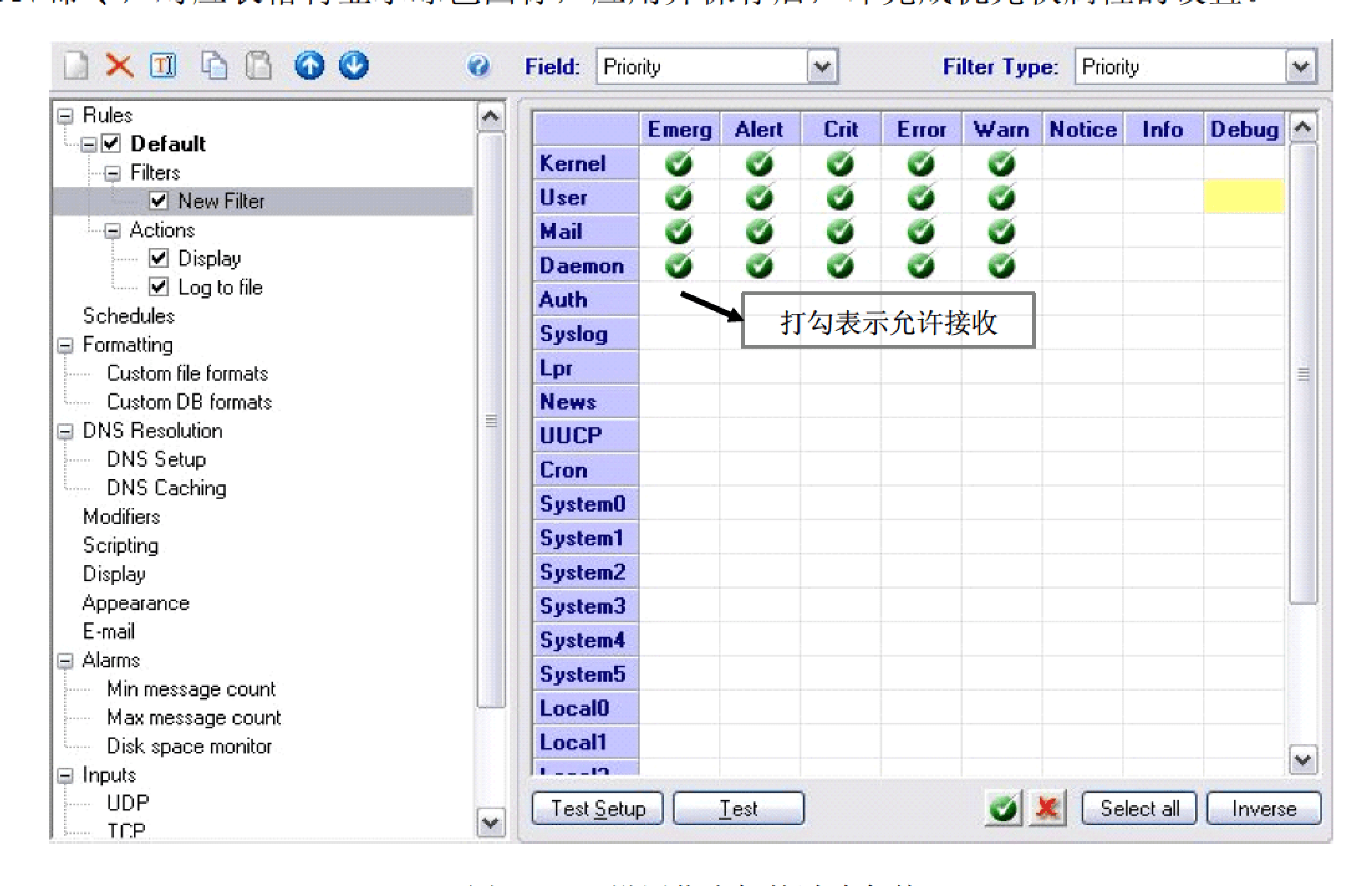


图 12-17　设置优先权的过滤条件

上述过滤条件描述为：任何由子系统 Deamon、Mail、User、Kernel 生成的，级别为 Warning 及其以上级别的日志信息，均可通过 Kiwi 接收并显示。

如果只关心系统守护进程子系统产生的日志信息，则只选择 Deamon 行即可，如图 12-18 所示。过滤条件可描述为，由子系统 Deamon 产生的任何级别的日志信息均可通过 Kiwi 接收和显示。

	Emerg	Alert	Crit	Error	Warn	Notice	Info	Debug
Kernel								
User								
Mail								
Daemon	✓	✓	✓	✓	✓	✓	✓	✓
Auth								
Syslog								

图 12-18　设置接受 Deamon 子系统产生的日志

12.2.3　IP 地址段过滤方式

每一条日志信息中均包含信息来源 IP 地址，在该过滤方式中，通过设置 IP 地址段，实现接受或排除所选段的日志信息。该方式只能在注册版本中使用。

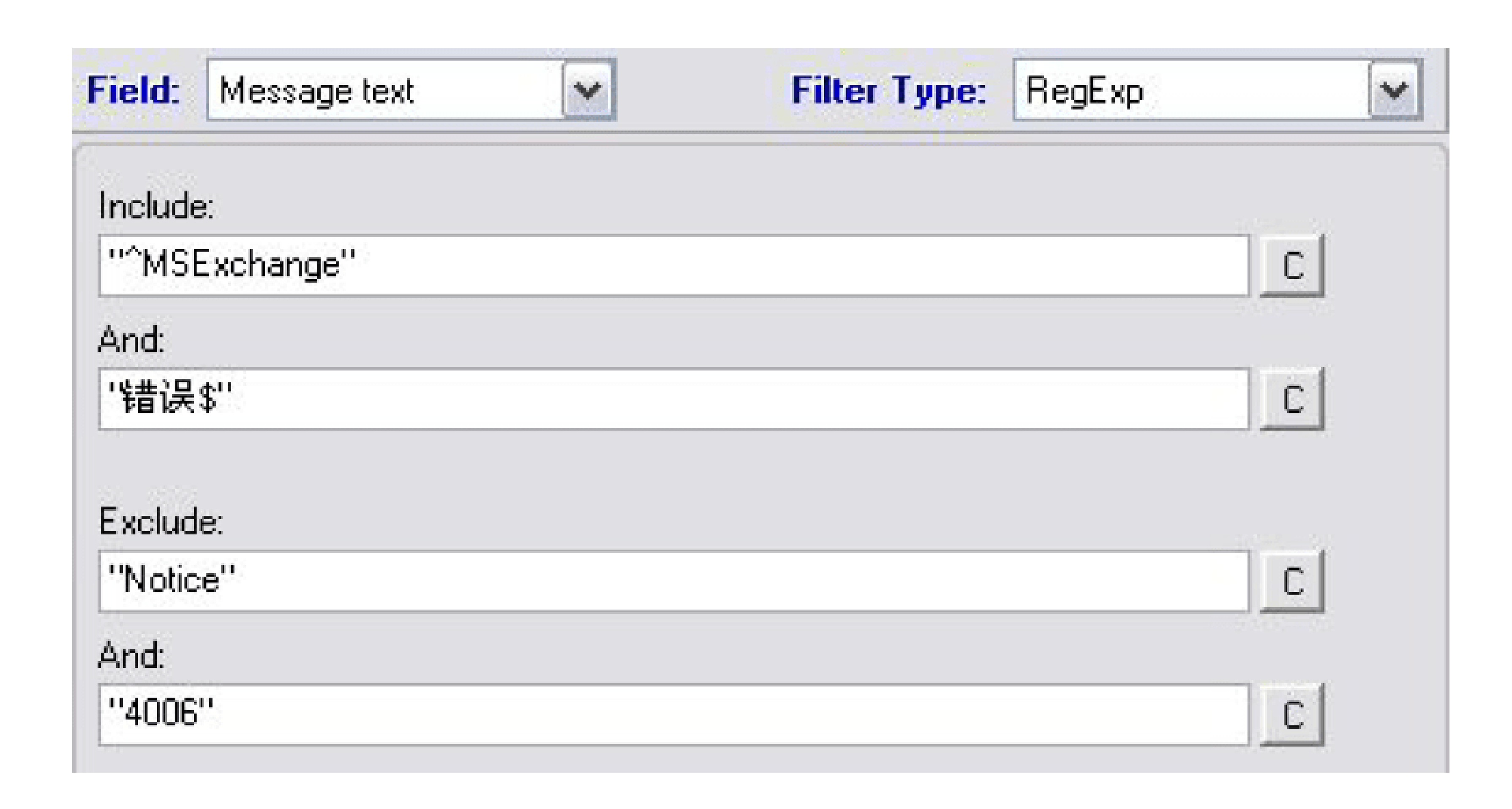


图 12-22 正则表达式字符串过滤方式

12.2.5 主机名过滤方式

该方式只能在注册版本中使用。与字符串过滤方式相似，同样可分为简单匹配、复合方式匹配和正则表达式匹配。只需要在文本框中输入要匹配的主机名称，并且用双引号标注，那么 Kiwi 程序将只接收来自于指定的主机设备产生的日志信息。

在过滤设置界面中新建过滤项，在 Field 选项中选择 Hostname，在 Filter Type 中选择 Simple，并输入设定的主机名，即完成该方式的过滤条件设置，如图 12-23 所示。



图 12-23 按主机名设置过滤条件

12.2.6 时间段过滤方式

时间段过滤方式，也就是设置允许接收日志信息的时段。只有在指定时段生成的日志信息才能够被程序接收和显示，否则被过滤掉。在过滤设置界面中新建过滤项，在 Field 选项中选择 Time of day，在 Filter Type 中选择 Time of day，并选择允许日志信息通过的时间段即可，如图 12-24 所示。

图 12-24 中的过滤条件描述为：在周一至周五的每天早 8:00-9:00 产生的日志信息能够被接收和显示。

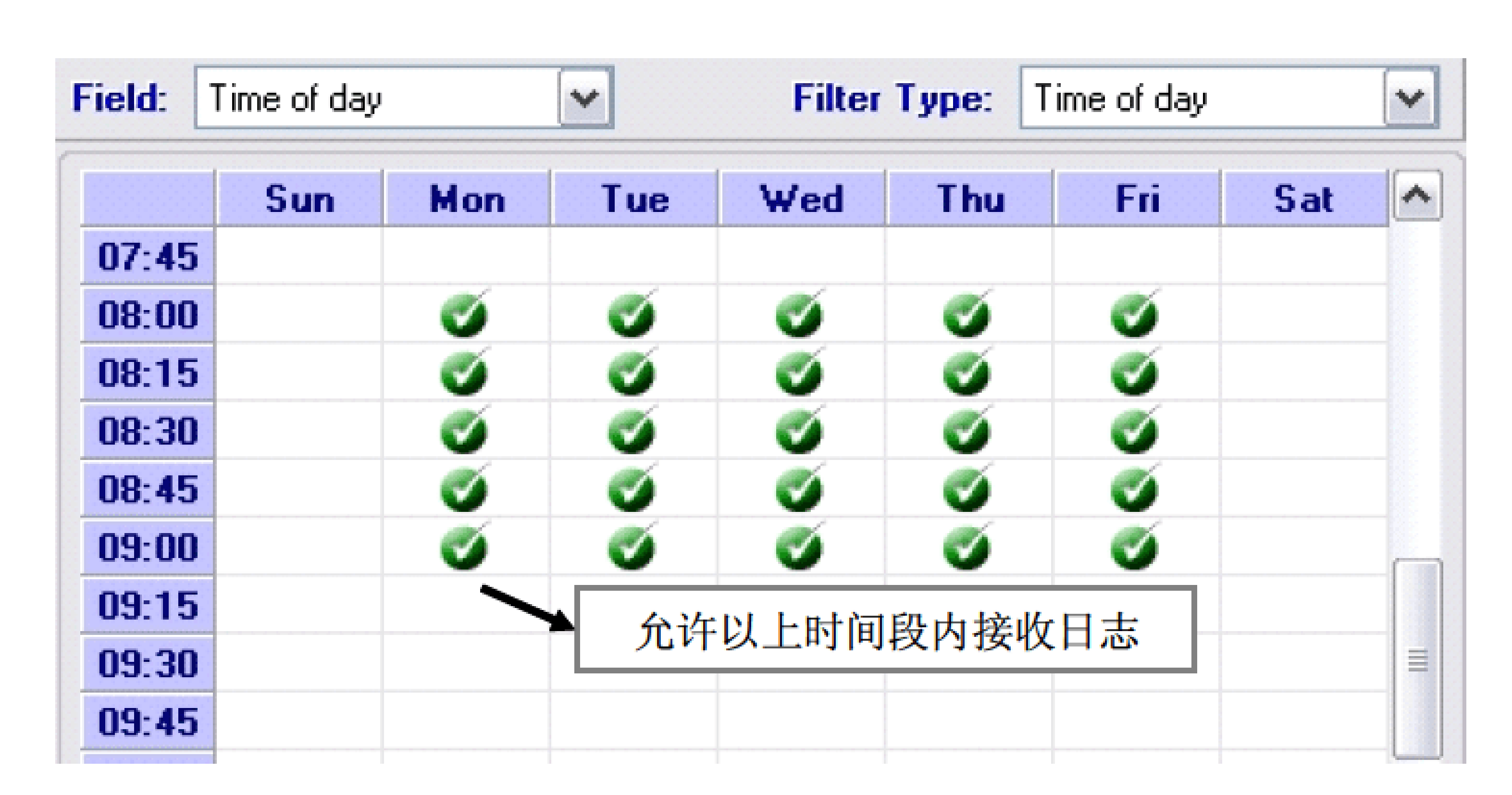


图 12-24　时间段过滤设置

12.2.7　时间间隔过滤方式

该过滤方式触发 1 次之后，将会等待设定的时间间隔之后，再次触发。并且该方式将会排在其他过滤方式之后，最后执行。时间间隔过滤包含 3 种方式：Time interval（时间间隔）、Threshold（阀值）和 Timeout（超时）。

该过滤方式适用于设定了提醒动作（如发送 E-mail）的情况下，当与设定内容匹配的日志信息反复出现时，将会触发生成大量的 E-mail 提醒邮件，为了减少提醒动作的执行，可设定时间间隔过滤，即发送邮件提示后，需要等待指定时间间隔后才会再次发送提醒邮件。

1．Time interval 过滤方式

在设置界面中新建过滤条件，在 Field 选项中选择 Flags/Counters，在 Filter Type 中选择 Time interval 选项，设定间隔时间后保存即可，如图 12-25 所示。

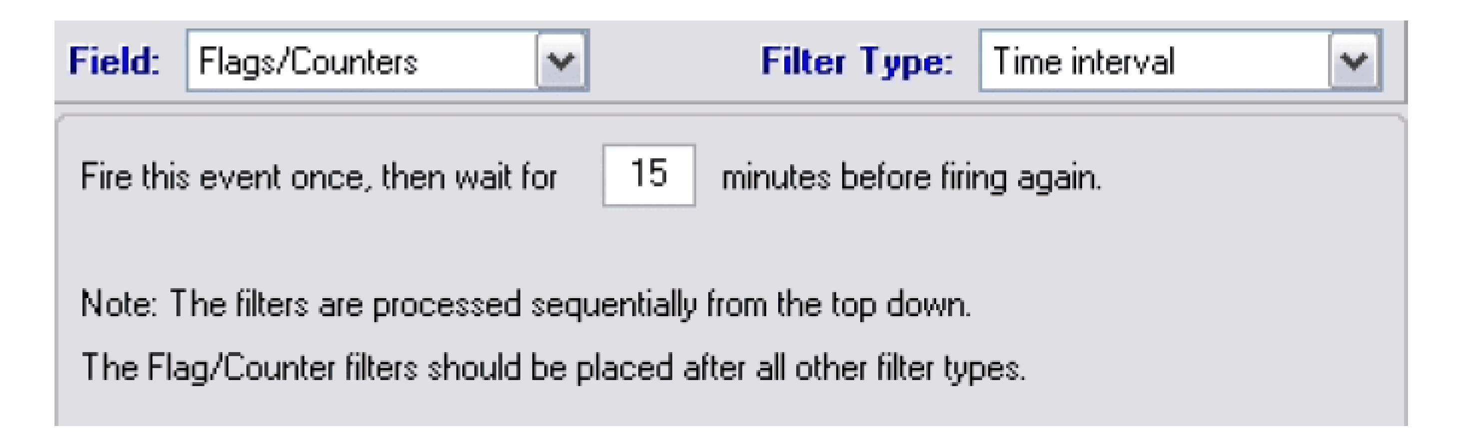


图 12-25　设置时间间隔过滤

举例：Kiwi 收到一条日志信息，包含了预设的 Link down 字符，文字匹配过滤方式返回 True，接着时间间隔过滤方式第一次执行，返回 True，那么报警动作将被触发执行。此时，Kiwi 再次接收到了该设备发出的包含 Link down 的日志信息，文字匹配过滤方式再次执行，同样返回 True，而时间间隔过滤方式需要 15 分钟之后才再次执行，于是返回结果 False，那么将不再触发执行邮件报警动作。

2．Threshold 过滤方式

在指定时间段内，其他过滤条件返回 True 的次数到达了指定阈值，那么将执行报警提

12.3 属性设置——执行动作

Kiwi 在接收日志信息时，默认执行两个报警提示动作，即显示和保存日志信息到 Text 文本中。除此之外，Kiwi 还提供了多种提示动作，例如，发送 E-mail 邮件提示、触发声音提示、存储日志信息到数据库中等以下分别介绍。

12.3.1 Display 显示日志

Kiwi 提供了 10 个虚拟显示界面，通过下拉菜单选择用于显示日志信息的虚拟显示器，并自定义该虚拟显示器的名称。

在设置界面中打开 Rules 页面，选择 Actions | Dispaly 选项，即可通过下拉菜单更换虚拟显示器，如图 12-29 所示。

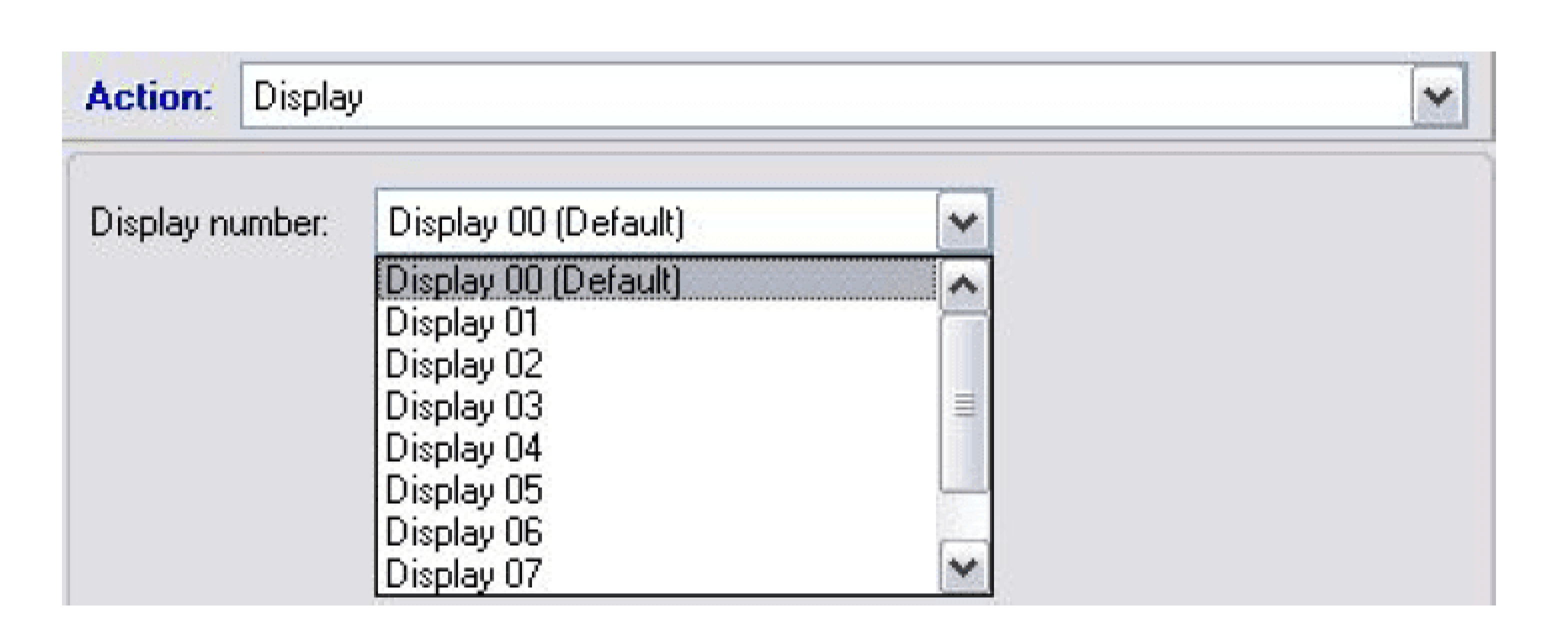


图 12-29　选择虚拟显示器

12.3.2 Log to file 保存日志

Kiwi Syslog 接收到日志信息后，将保存日志信息到文本文件中。默认该文件位于程序安装目录（InstallPath\Logs）的文件夹中，文件名为 SyslogCatchAll.txt。

在 Rules | Actions | Log to file 设置界面中，可更改保存文件的路径、文件名和格式，如图 12-30 所示。

在 Log file format 下拉列表中，提供了多种保存日志信息的格式。默认的日志信息存储格式为：DateTime（YYYY-MM-DD HH:MM:SS）[TAB] Priority （Facility.Level） [TAB] Host name [TAB] Message text。

在设置界面下方的 Log file Rotation 区域中，可设置保存日志文件的大小或时长，以防止日志文件无限制地增长，导致磁盘空间的浪费。

Maximum log file size 文本框可设置单个日志文件的最大容量。Maximum log file age 为设置文件保存的时长。当一个日志文件到达指定的容量限制或时长后，当前日志文件将被命令为另外一个名称（如 logfile.txt.001），并存储到一个新建的空文件中，当空文件再次达到阈值时，logfile.txt.001 更名为 logfile.txt.002，当然日志文件更名为 logfile.txt.001。以此类推，当文件数量到达指定的 12 个时，最早生成的日志文件将被删除。



图 12-30　设置日志文件保存目录等

12.3.3　转发日志文件

转发日志文件执行动作将日志服务器接收到的日志信息通过 TCP 或 UDP 协议将日志记录转发到另外一台日志服务器中。当网络中存在多个日志服务器，并需要将各日志服务器中的信息进行转发汇总时，可使用该功能。

在 Rules | Actions 页面单击新建按钮，并在 Action 下拉列表中选择 Forward to another host 选项，设置选项后，可实现转发日志信息的功能，如图 12-31 所示。

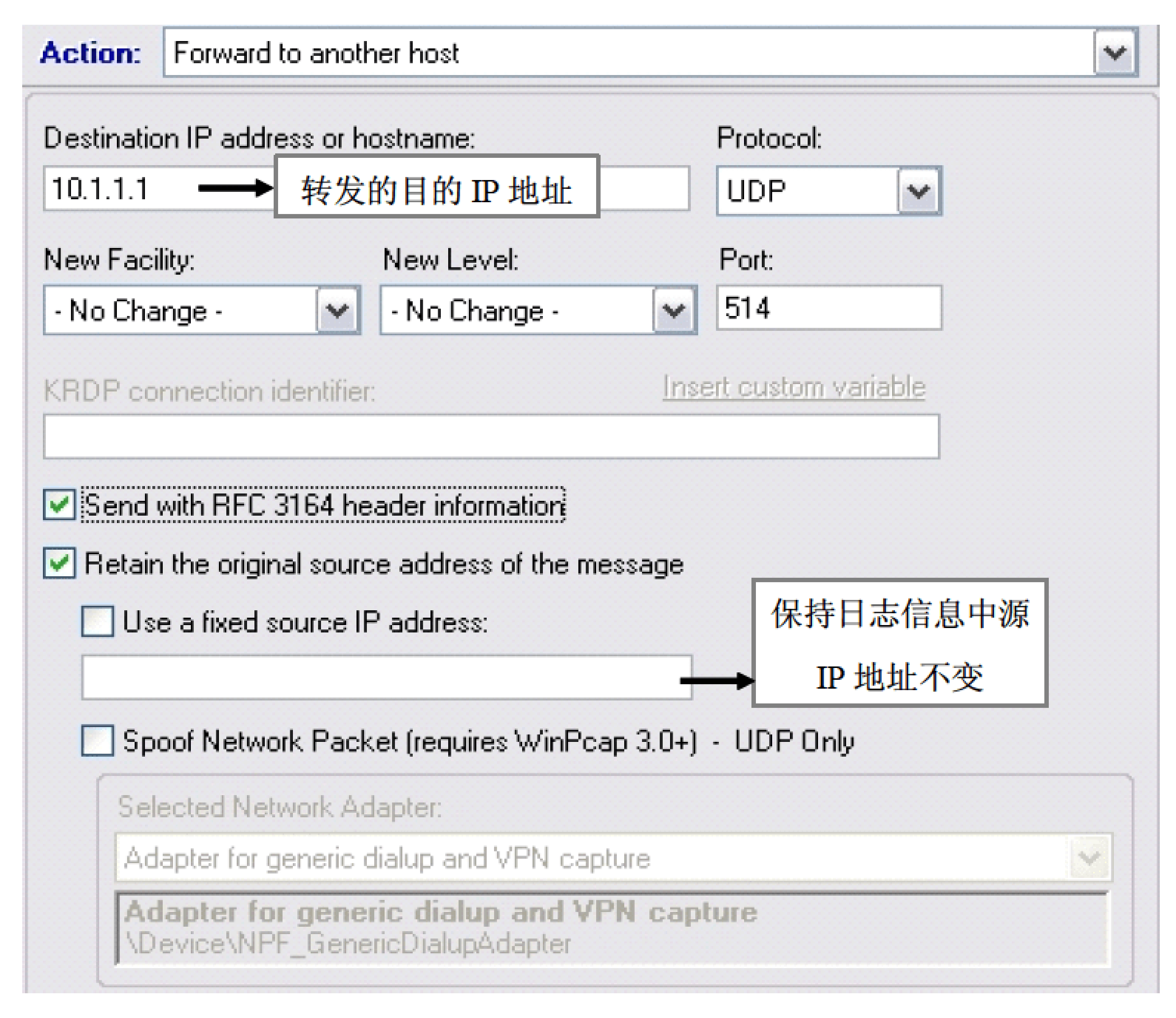


图 12-31　设置转发日志信息至其他日志服务器

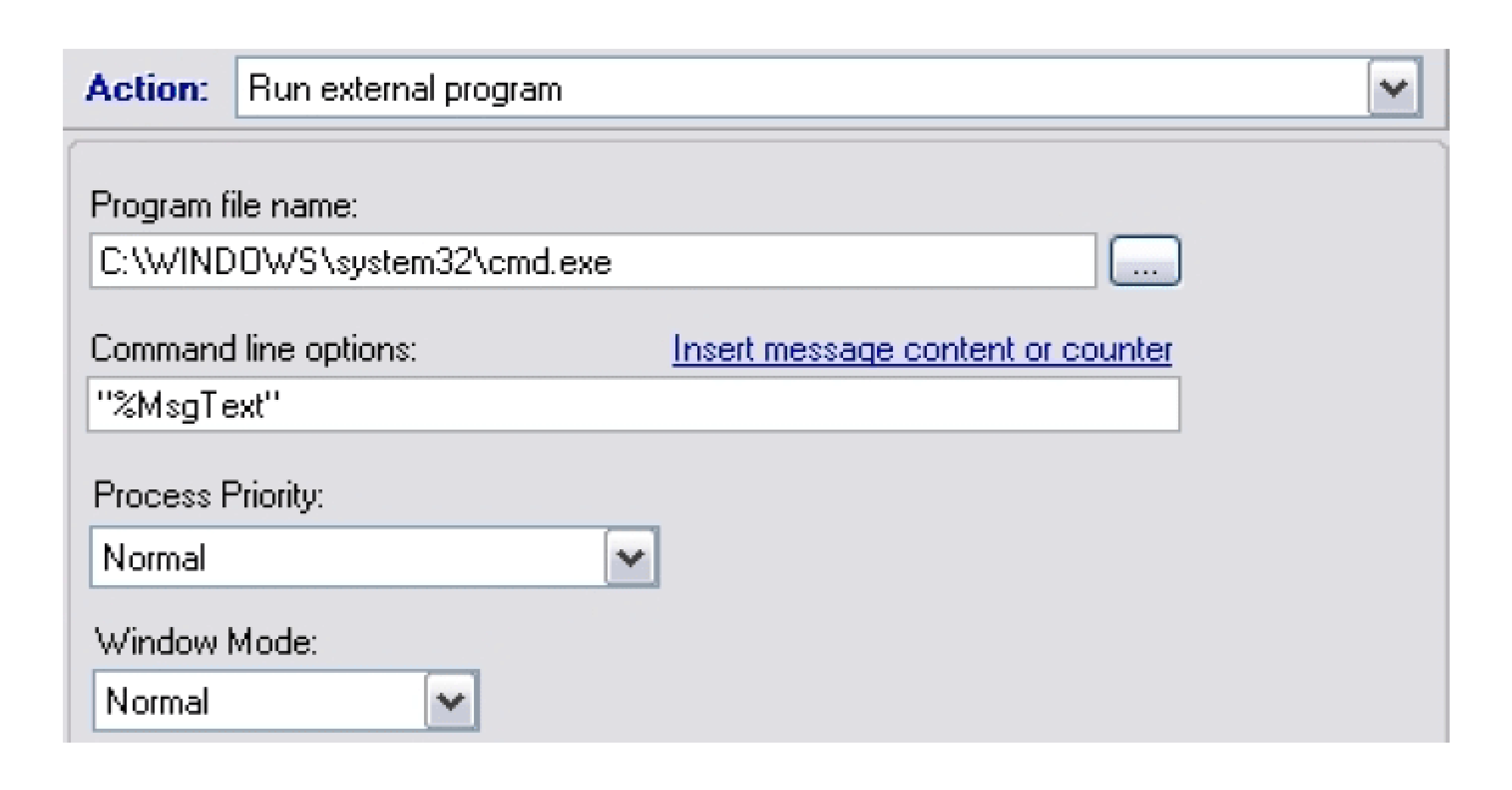


图 12-33 设置调用外部程序

12.3.6 发送 E-mail 报警信息

发送 E-mail 报警信息能够将接收到的日志信息内容通过 E-mail 发送至指定邮箱，日志信息的详细内容和统计等信息也能够包含在邮件内容中。设置步骤如下：

（1）设置 E-mail 接收地址及邮件内容之前，首先需要设置 Kiwi 找到正确的邮件服务器地址，在设置界面中选择左侧树状菜单的 E-mail 选项，打开 E-mail 设置界面，如图 12-34 所示。

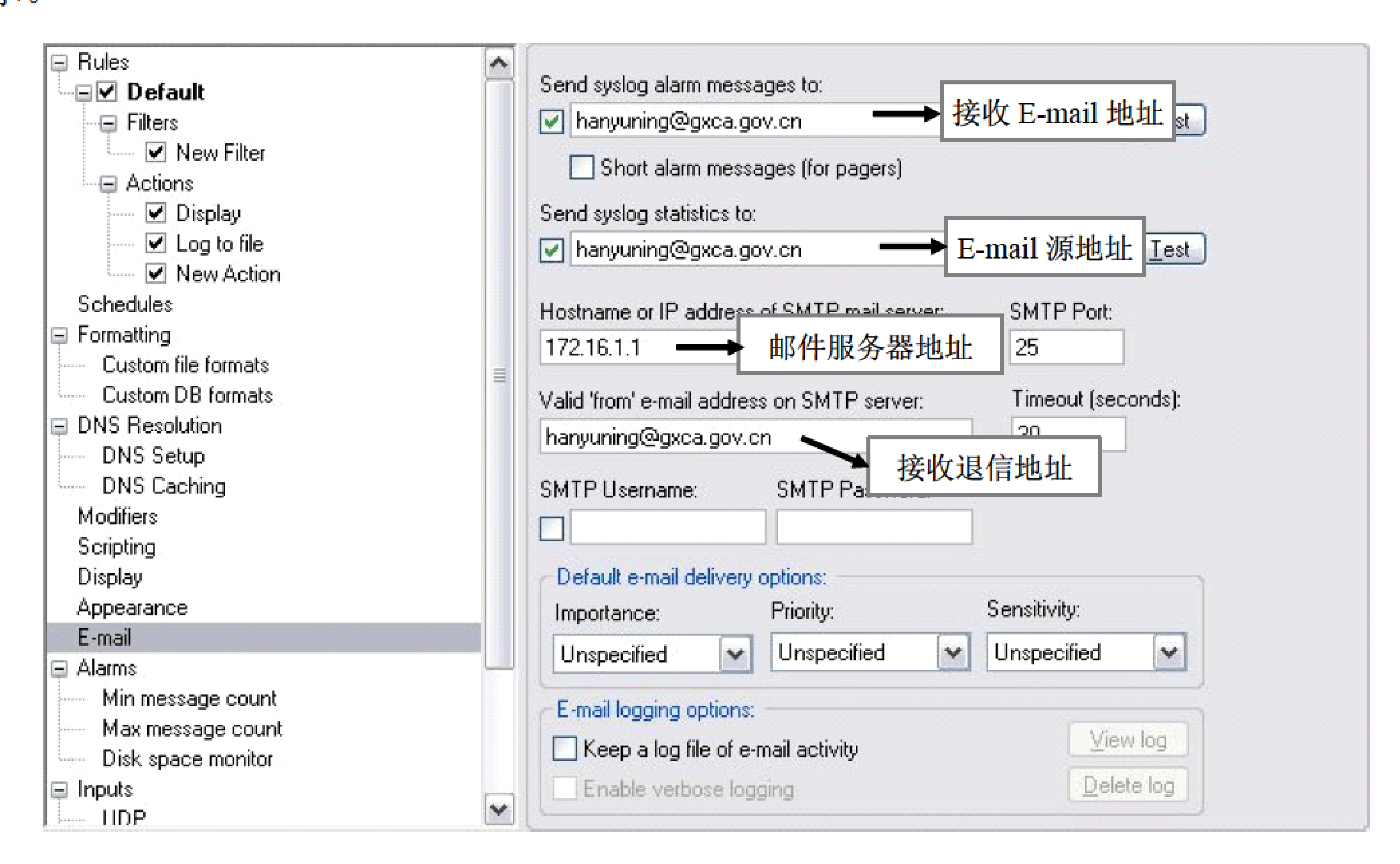


图 12-34 设置 E-mail 发送

- ❑ Send daily statistics via e-mail to：设置接收 E-mail 报警信息的 E-mail 邮箱地址，例如 Test@company.com。
- ❑ Hostname or IP address of SMTP mail server：设置 SMTP 邮件服务器的 IP 地址。

12.3.7 发送日志信息

发送日志信息用于在接收到日志信息时，生成一条 Syslog 提示信息并发送至指定的服务器中，该信息可包含额外的细节信息或自定义添加的信息。

在该设置界面中，需要设置接收信息的服务器 IP 地址，以及选择需要包含的额外信息，如图 12-37 所示。



图 12-37 设置接收日志信息时发送提示信息

12.3.8 记录日志信息至数据库

当接收的日志信息越来越多时，将生成较大容量的文本文件，将造成空间的浪费和查询的困难。此时可考虑将数据存储到数据库中。Kiwi Syslog 是通过数据源（ODBC）连接数据库，默认支持 Access、SQL Server、MySQL 和 Oracle 四种类型的数据库。

选择数据库类型后，还需建立数据表，这 4 种数据库均默认建立包含同样字段的表结构，字段分别为 Date、Time、Priority、Hostname 和 Message text 五个字段。

以下以 MS Access 数据库为例进行介绍，步骤如下：

（1）先在 Access 程序中新建一个数据库，并将库文件保存至任意目录。

（2）在设置界面 Rules | Actions 选项下新建一个类型为 Log to Database 的执行动作，如图 12-38 所示。

在如图 12-38 所示的界面中，需在 Data link connection string 文本框中添加数据源。单击浏览按钮，在弹出的数据源设置界面中选择 Microsoft Jet4.0 OLE DB Provider（即选择连接 Access 数据库），然后选择刚才新建的 Access 库文件，单击“测试连接”按钮，如果提示连接正常，则完成设置，如图 12-39 所示。

（3）返回 Log to Database 设置界面中，并单击 Create table 按钮，进行自动建表，如果提示成功，将会在 Access 数据库中自动生成一个命名为 Syslogd 的数据表。

（4）设置后，日志信息将自动存储至该 Access 数据库中。如需要查询数据，可单击 Query table 按钮进行查看。

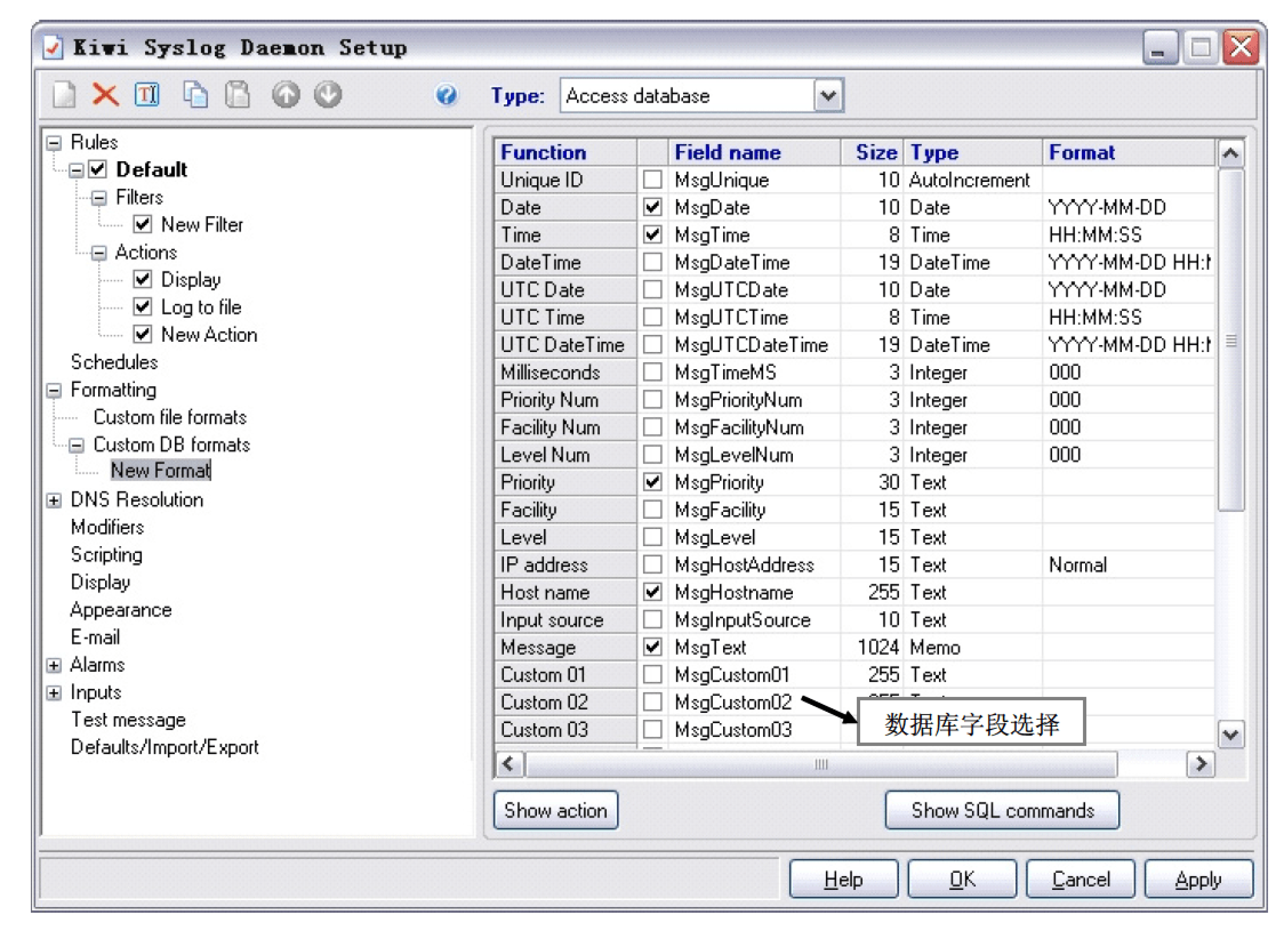


图 12-40　设置数据库字段

12.3.9　记录日志为 NT 系统应用程序事件

该动作可将接收到的日志信息记录到 Windows NT 系统中的应用程序事件记录中。NT 系统日志包括 5 种级别，分为 Error、Warning、Information、Success 和 Failure。

在 Log to NT event log 设置界面中，可在 Event log message type 下拉列表中选择日志类型，Kiwi 接收到的日志信息将存储为所选类型，如图 12-41 所示。

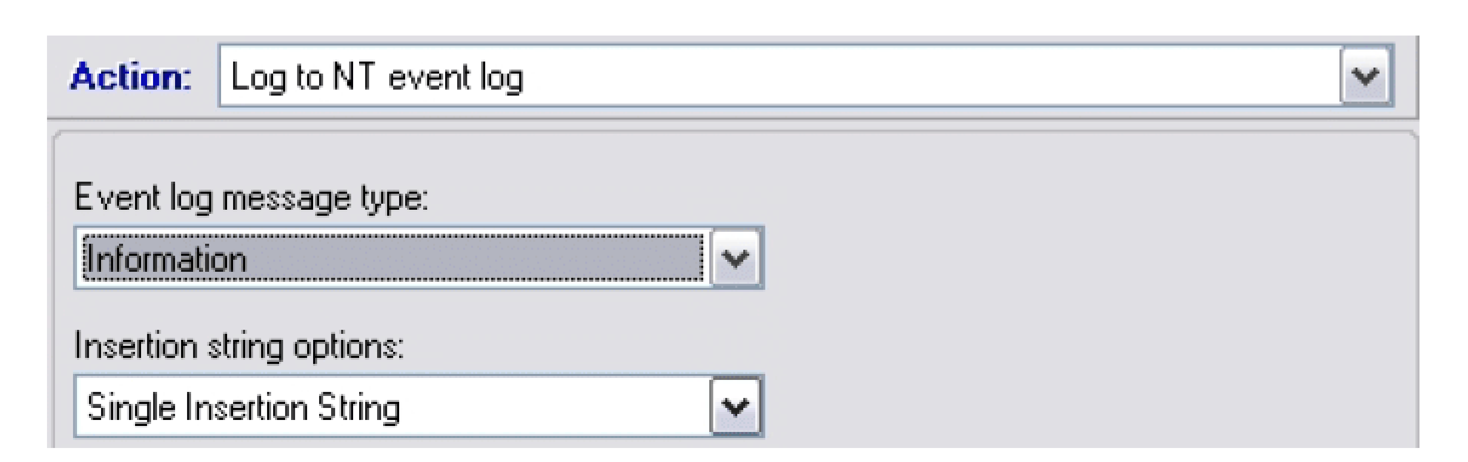


图 12-41　记录日志到 NT 应用程序事件中

12.3.10　发送 SNMP trap 信息

接收日志信息时，发送 SNMP Trap 信息至指定的 IP 地址，如果目的 IP 主机包含监听

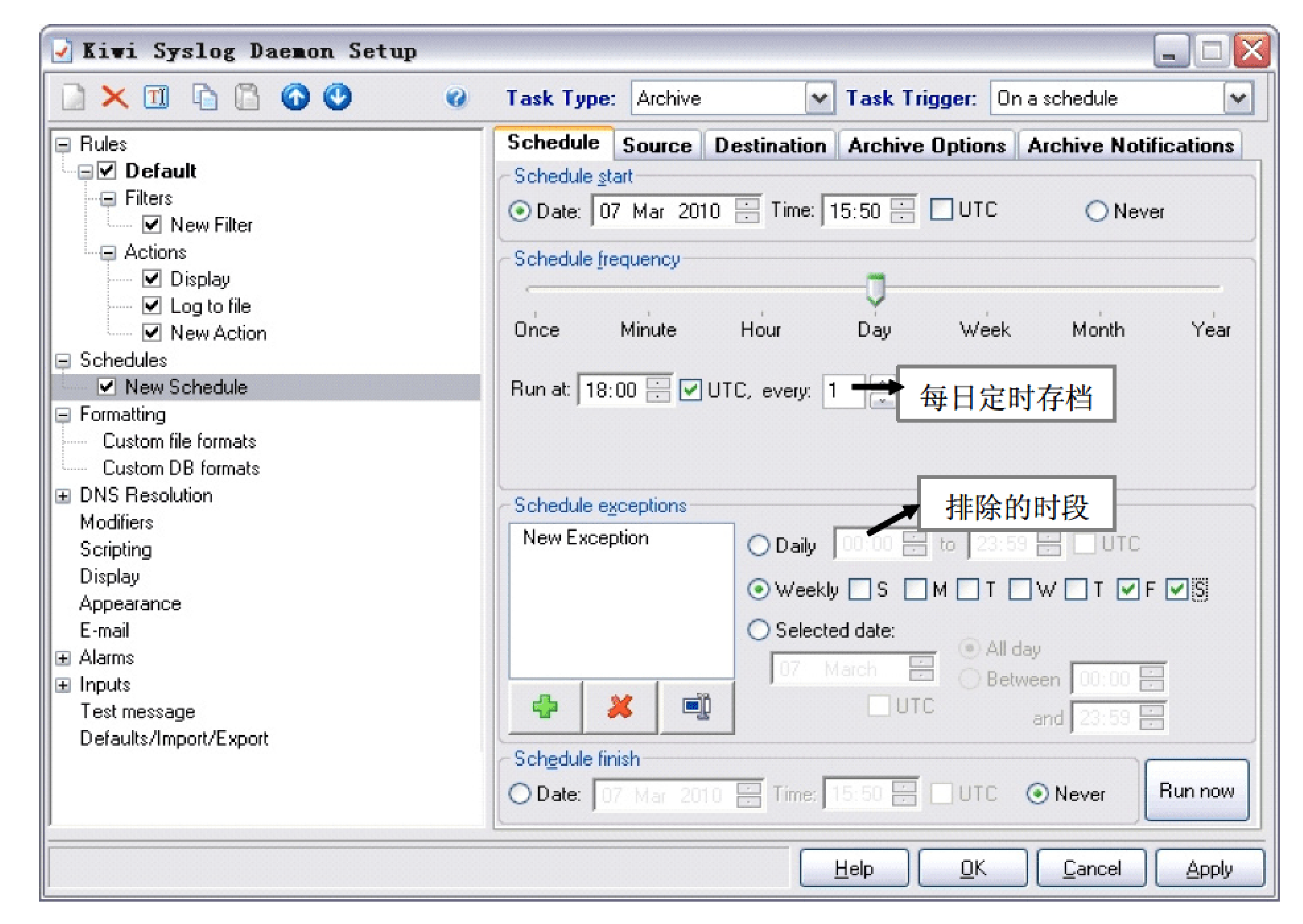


图 12-44　新建存档日程安排表

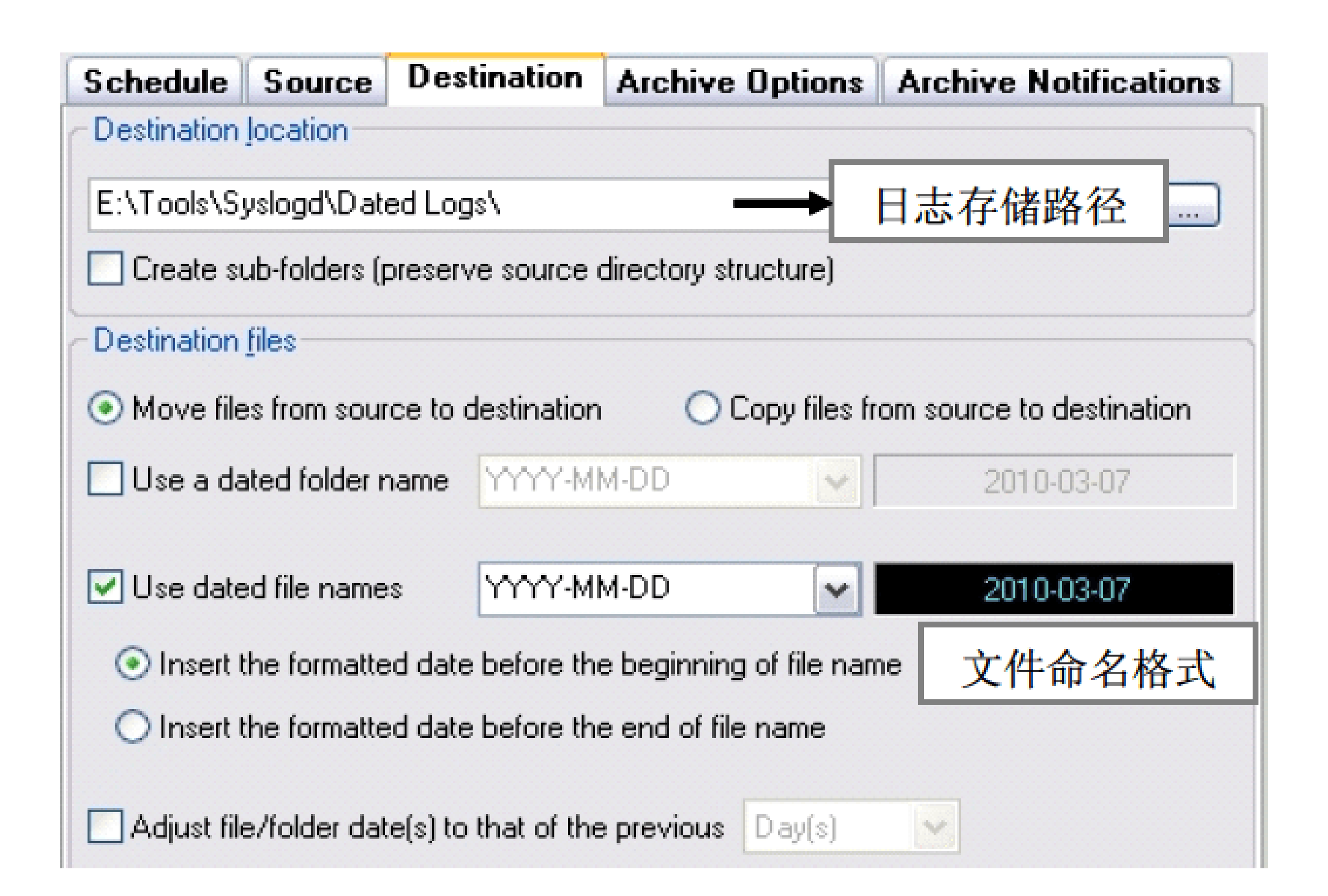


图 12-45　选择要存档的文件和存储位置

Archive Notification 页面：用于设置发送存档情况的提示信息，可选择将存档情况以 HTML 格式或纯文本格式发送至指定邮箱。此处选择按照 HTML 方式发送信息至 Managerz@gxca.gov.cn 邮箱，如图 12-47 所示。

12.4.2　设置日志存储格式

该选项包含 Custom file formats 和 Custom DB formats 两个设置项，分别用于设置记录日志信息到文本文件的格式和记录日志到数据库的格式，主要是设置包含的字段。日志存

储到数据库中的字段在 12.3.8 小节记录日志信息至数据库中已经做过介绍。此处介绍设置文本记录的格式。

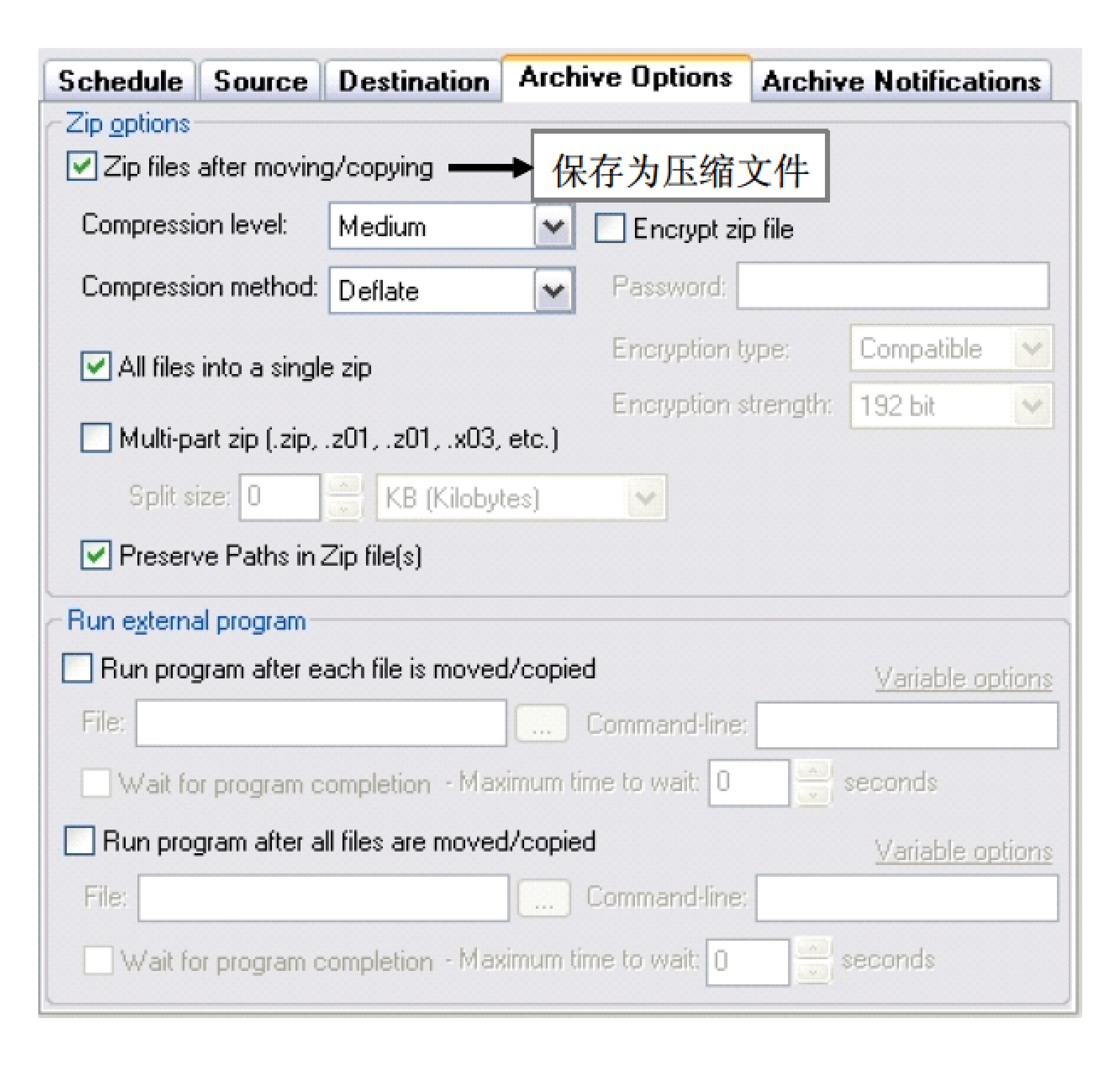


图 12-46　设置存档属性

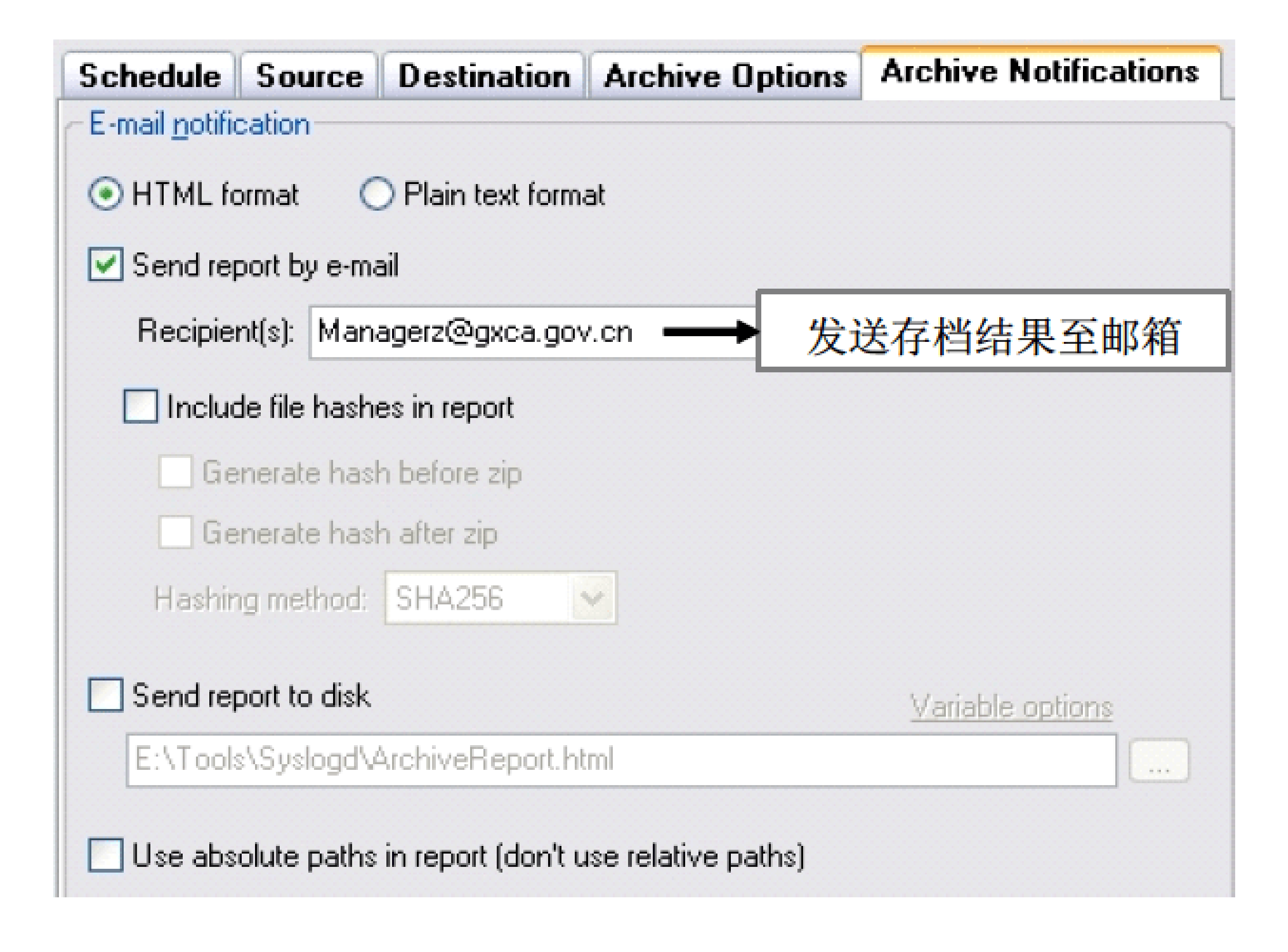


图 12-47　设置发送存档结果至指定邮箱

默认 Kiwi 在记录日志信息到 Text 文本中时包含了 5 个字段，分别是日期、时间、日志产生的子系统、主机名和日志信息内容。如果需要添加更多的记录字段，或按照自定义格式存储信息，可通过该设置实现。

在设置界面的 Formatting | Custom file formats 选项页面中单击新建按钮，将建立一个新的文本格式，选择要添加的字段、时间显示样式和字段排序即可，如图 12-48 所示。

设置完成后在 Rule | Actions | Log to file 选项中选择 Log file format 下拉列表，将看到刚才新建的自定义文本格式，选择该格式后，日志将按此格式进行存储，如图 12-49 所示。

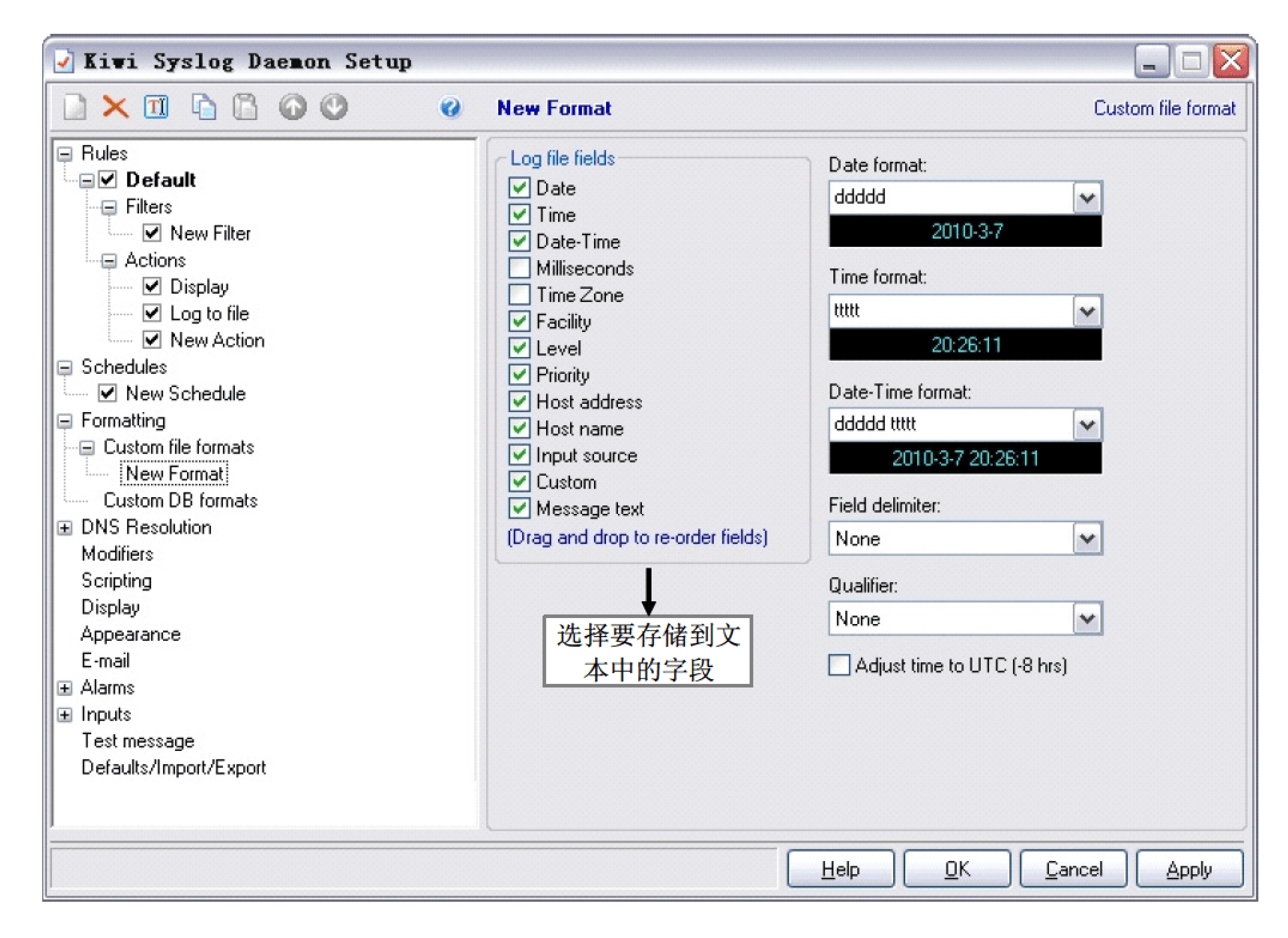


图 12-48 设置记录日志信息的文本格式

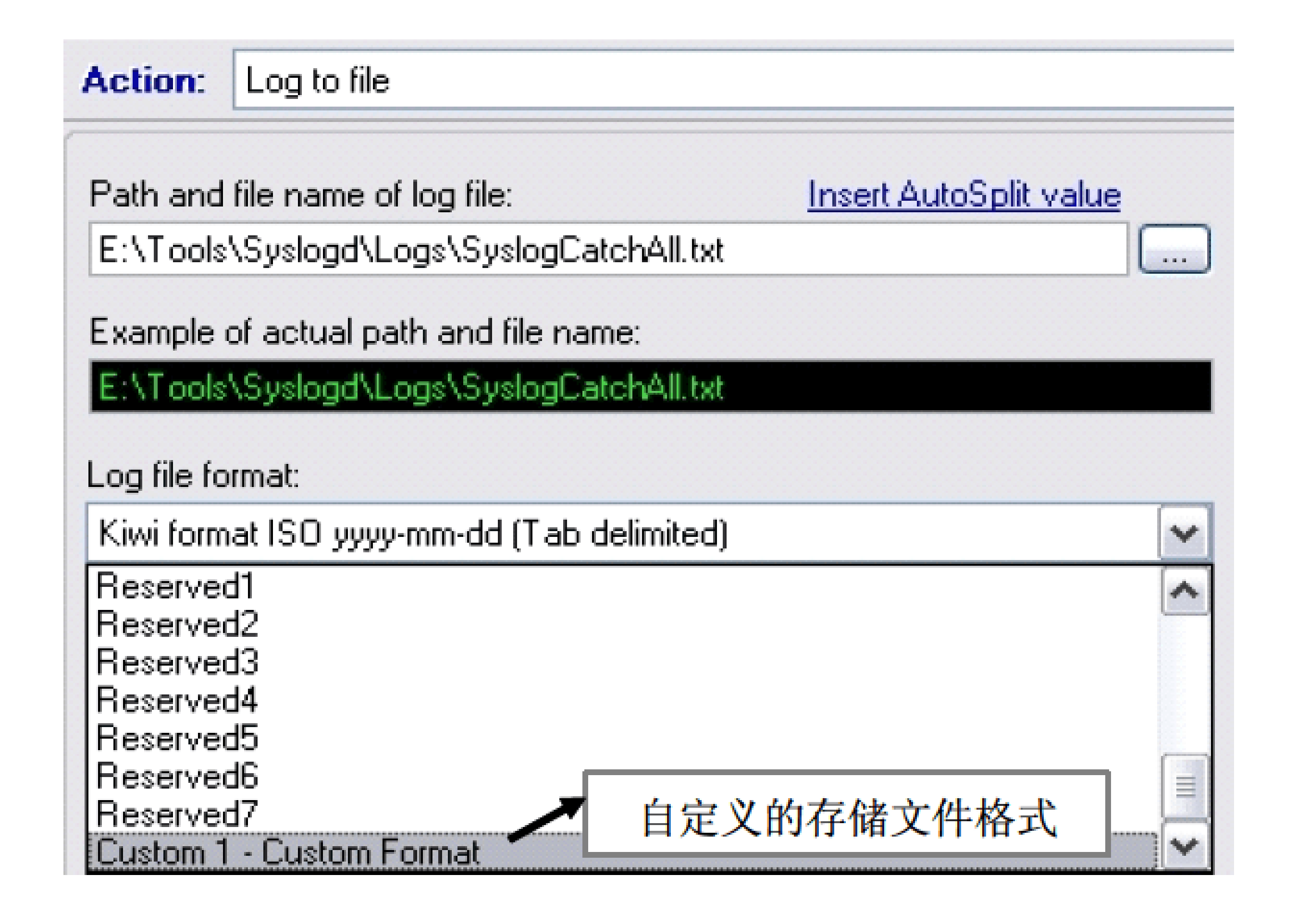


图 12-49 选用自定义的文本格式

12.4.3 DNS 解析设置

在接收 Web 服务器或防火墙等设备时，发送信息的主机及日志信息的内容中都有可能包含 IP 地址。通过该项设置，可对这些 IP 地址进行解析，转换为易读的名称或网址。例如，可将 IP 地址 58.63.236.26 解析为网址 www.sina.com.cn。

在设置界面中，选择 DNS Resolution 选项，在该界面中选中 Resolve the IP address of the



图 12-52 设置触发报警的最低阈值

12.4.7 输入设置

输入设置可设置 Kiwi 通过 3 种方式对日志信息进行监听和接收，分别是监听 UDP 端口、TCP 端口和 SNMP trap 陷井信息。默认 Kiwi 程序允许监听 UPD 的 514 端口，该协议和端口为最常用的日志信息发送端口。

有些防火墙（如 Cisco PIX）和 Syslog 设备通过 TCP 端口发送日志信息。默认通过 TCP 发送日志信息的端口为 1468，Kiwi 中默认开启对该端口的监听。

SNMP Trap 信息默认通过 UDP 协议的 162 端口发送信息。Kiwi 中默认未开启对 Trap 信息的监听。

1．UDP 监听设置

选择 Inputs | UDP 选项，打开 UDP 监听设置界面。如果需要停止接收日志 UDP 协议的日志信息，只需要取消 Listen for UDP Syslog Message 的选中，即可停止对 UDP 端口的监听。该界面还允许修改监听 UDP 协议的端口，但更改端口后，只能够接收到支持指定端口的日志信息。

Bind to address 用于绑定接收日志信息的网卡接口。默认 Kiwi 将接收系统中多个网卡接收的日志信息，如制定了绑定的网卡，那么将只接收来自该网卡的日志信息，如图 12-53 所示。

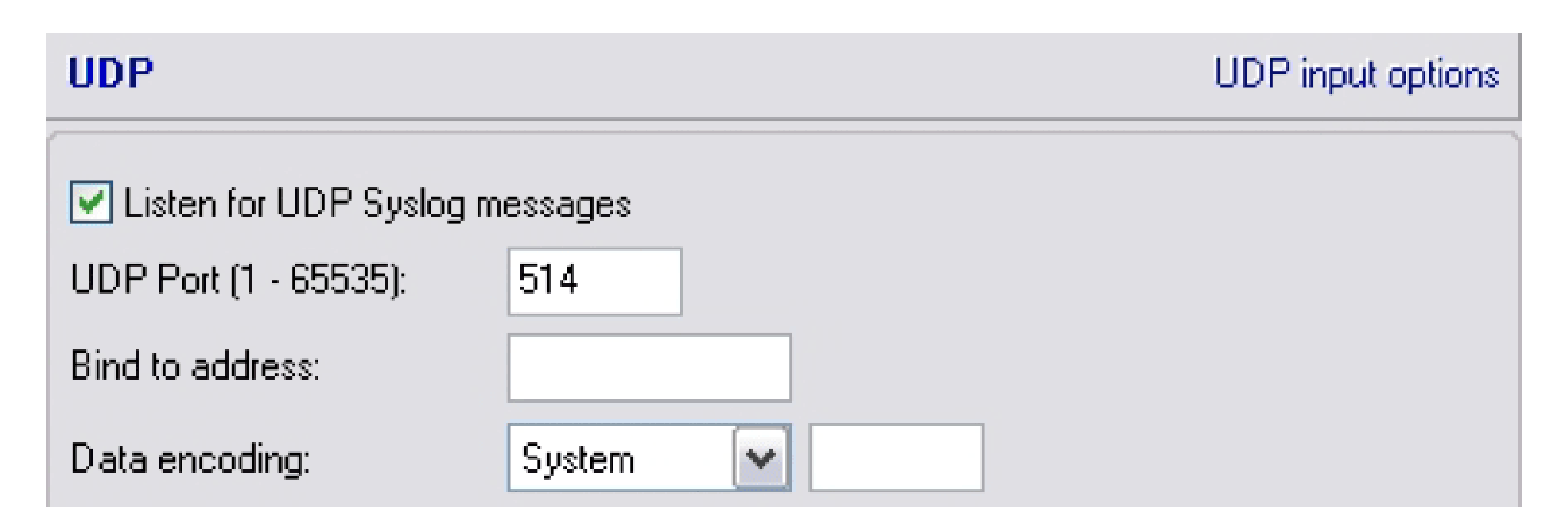


图 12-53 设置 UDP 监听属性

找故障的原因；

- 有可能是其他应用程序占用了 Kiwi 程序接收日志信息的 UDP 端口，关闭该程序并重启 Kiwi 程序。

开启 Windows 防火墙对 Kiwi 监听端口的阻止，步骤如下：

（1）打开控制面板｜Windows 防火墙，并打开“例外”选项卡，在该界面中列出了 Windows 防火墙放行的端口，如图 12-55 所示。

（2）单击添加端口按钮，并将 Kiwi 程序默认监听的端口 UDP 514 添加到列表中，如图 12-56 所示。



图 12-55　设置 Windows 防火墙



图 12-56　设置 Windows 防火墙放行的端口

通过以上步骤的检查和操作，能够排除日常的 Kiwi 程序故障，保证日志信息的正常接收和保存。

Kiwi SyslogGen 是专门用于发送 Syslog 测试信息的免费工具，它发送标准 Unix 类型的 Syslog 信息至任何 PC 或 Unix 日志服务器。支持 TCP 端口发送的测试信息，用于测试 Kiwi Syslog Deamon 服务配置是否正常运行。

从 Kiwi Syslog 的官方网站（www.kiwisyslog.com）可以获取该程序。

12.6　Kiwi 辅助工具介绍

12.6.1　Kiwi SyslogGen 简介

- 该程序使用 UDP 和 TCP 协议发送测试信息；
- 包含各种优先权类型的日志供发送，可发送预设的消息或自定义的消息内容；



图 12-61　Kiwi SyslogGen 的简洁界面

12.6.3　Kiwi Syslog Viewer 简介

只有在 Kiwi Syslog 注册版本中，才提供高亮色彩显示日志信息的功能。通过配色方案查看日志，能够让各类日志信息一目了然。Kiwi Syslog 接收到的日志信息都是存储在 Text 文本中，当数据量较大时，查看和检索信息都极不方便。

Kiwi Syslog 程序还提供了辅助查看日志信息的工具 Kiwi Syslog Viewer。该工具提供了显示配色方案、查找、过滤等功能，在查看 Text 文本日志信息时尤为方便。打开 Text 文本日志信息后，Syslog Viewer 界面如图 12-62 所示。

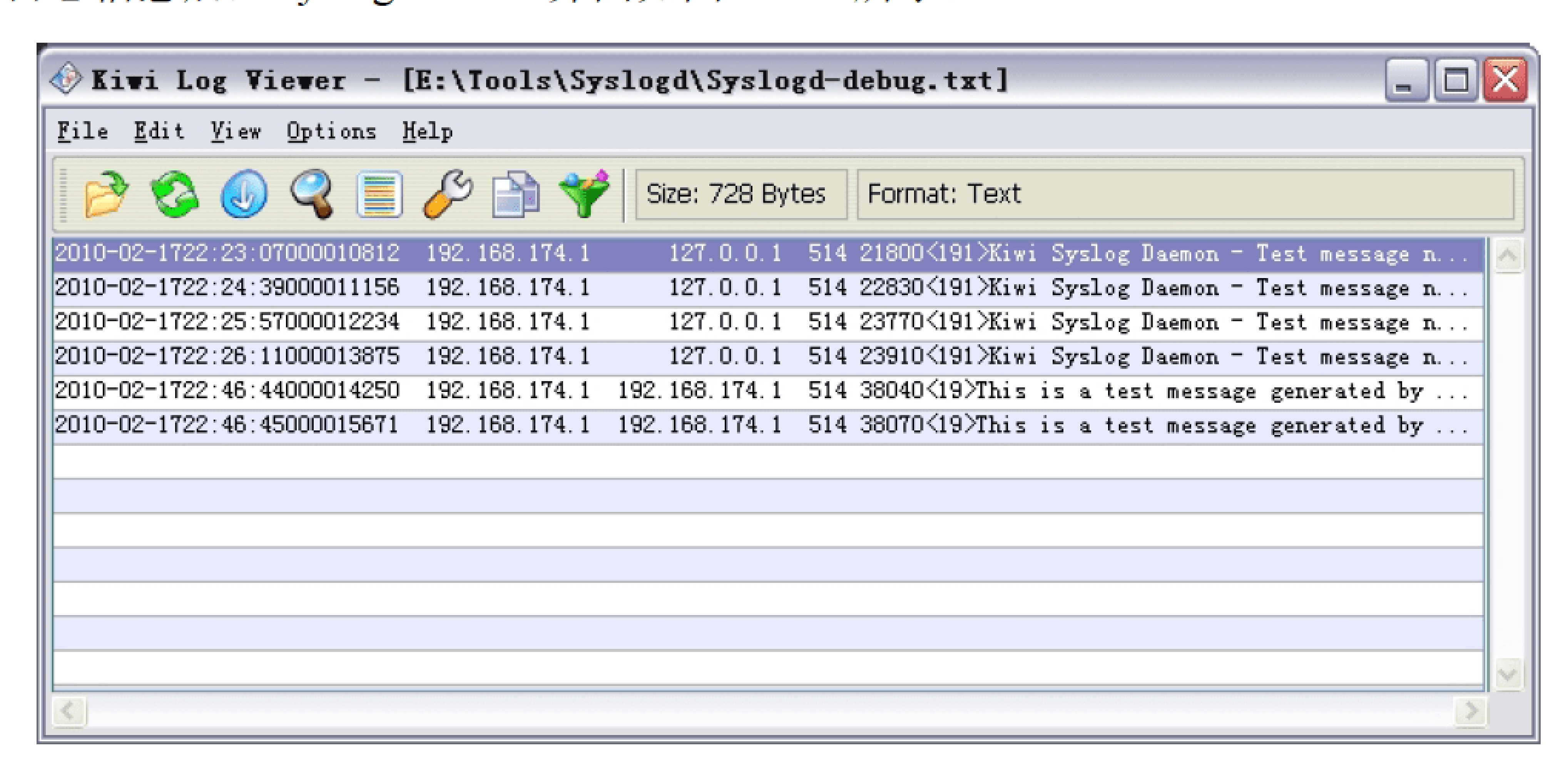


图 12-62　Kiwi Syslog Viewer 程序界面

12.6.4　Kiwi Syslog Viewer 配置和使用

1．设置配色方案

选择菜单中的 Options | Highlighting 命令，或单击快捷按钮，可打开按配色分类显示日志信息的设置界面。在该界面中，单击按钮，可添加配色显示方案。只要日志内容中包含匹配的字符串，就可按照所选颜色分别显示字体颜色和背景颜色。配色设置如图 12-63 所示。

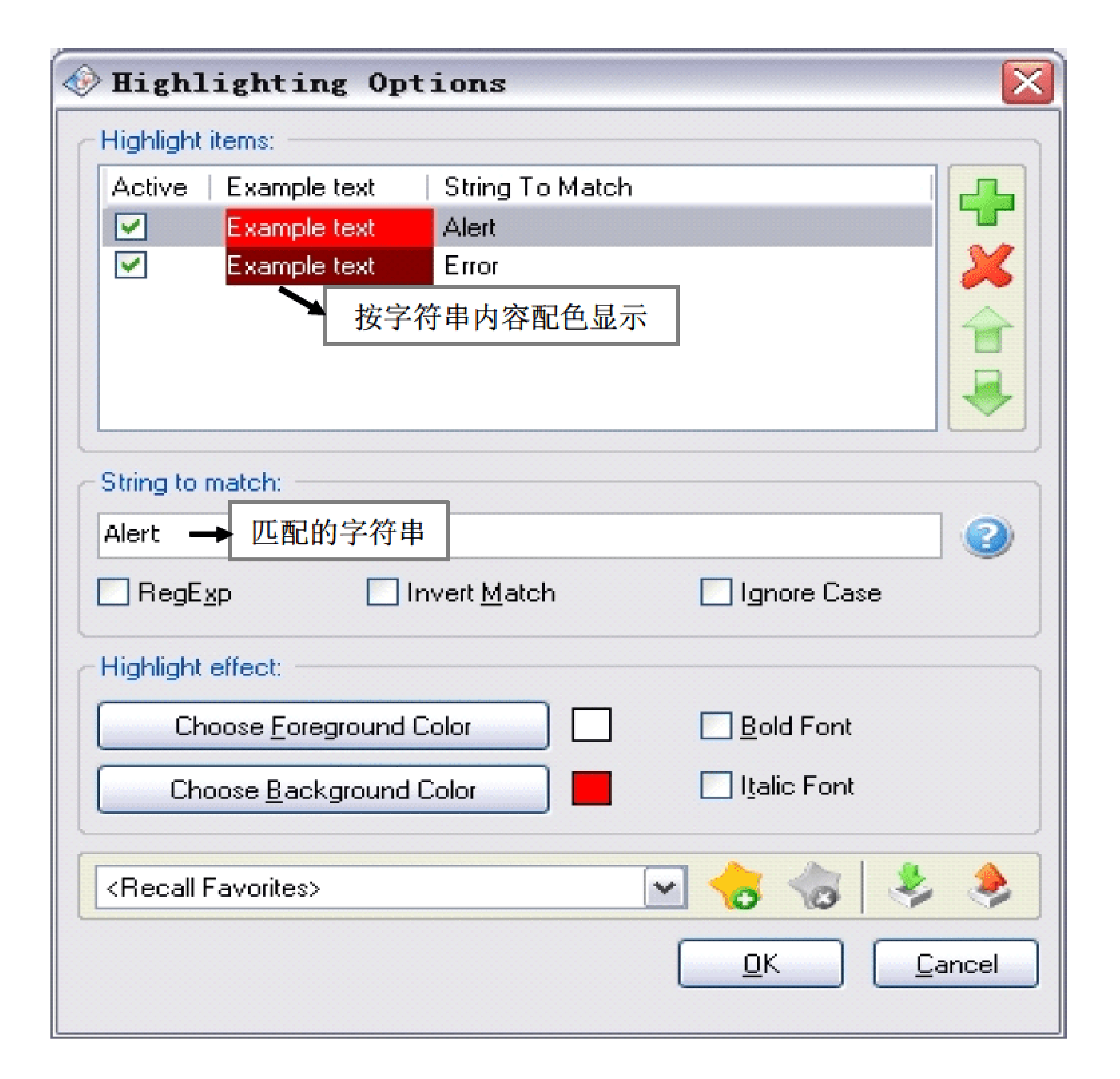


图 12-63　配色方案选择

配色方案包含 Alert 字符串，则信息字体颜色为白色，背景为红色；包含 Error 字符串，则字体颜色为白色，背景为暗红色，如图 12-64 所示。

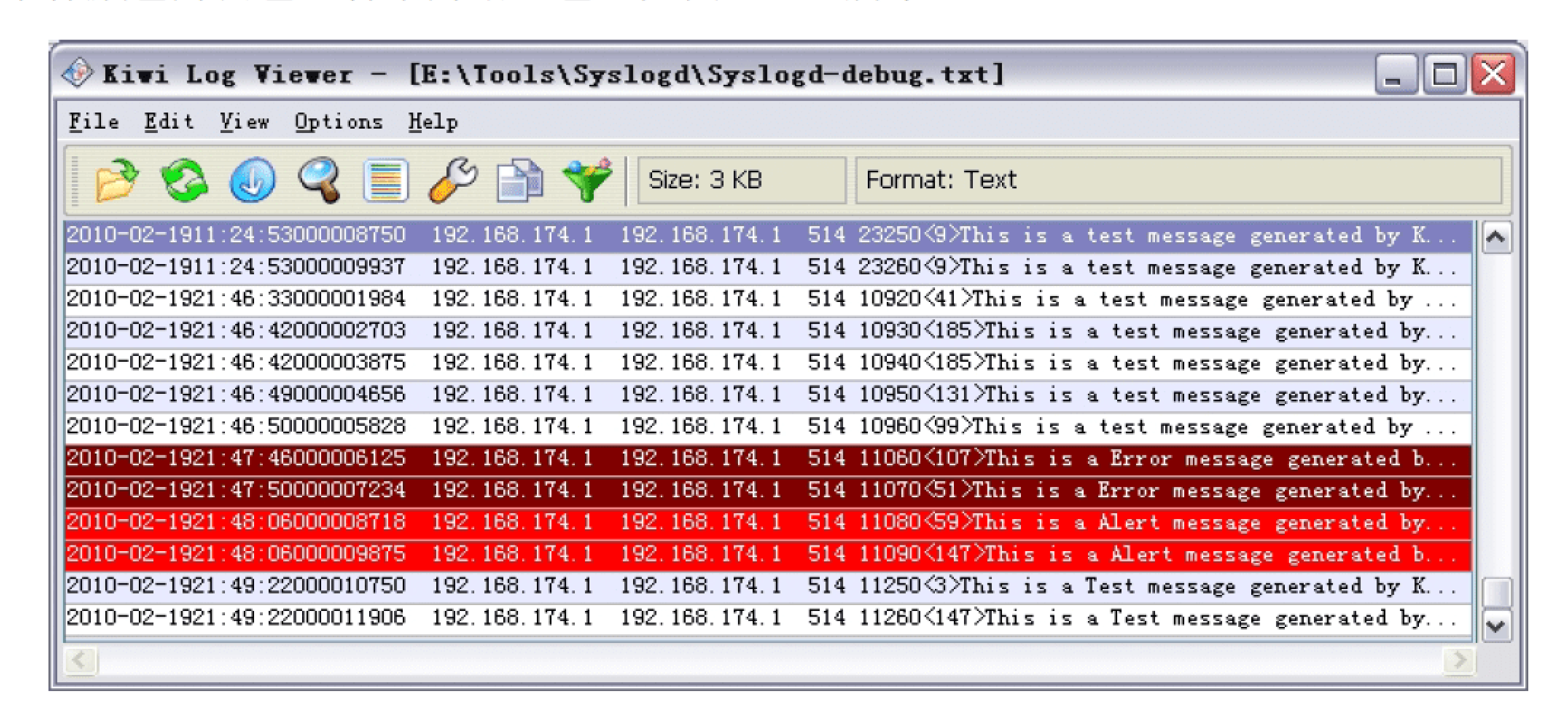


图 12-64　按配色查看日志信息

2．设置内容过滤

单击按钮，可打开过滤窗口，该窗口可根据所输入的字符串进行显示过滤，只显示与字符串匹配的日志信息，此处可输入日志类型、IP 地址等，如图 12-65 所示。

附录　MIBII 节点描述

表 1　MIBII System（接口）组节点描述

节点标识	对 象 名 称	对 象 描 述
（1）	Desc	只读的显示串，它是对实体的描述，包含所用硬件、操作系统和网络软件的名称和版本等完整信息。它显示为印刷体 ASCII 码字符
（2）	ObjectID	只读对象，SMI（管理信息结构）企业树中所包含的子系统的网络供应商标识
（3）	UpTime	只读的 TimeTicks 类型，它定义自最近一次重新启动网络管理软件所经历的时间（以 1/100 秒为单位）。通常 Agent（代理）在启动时便初始化时钟
（4）	Contact	可读写的显示串，它负责管理节点的联系人名字和联系地址信息，常用于测试 Agent 是否可写
（5）	Name	该被管理节点的指定名称，通常该名称具有管理节点的全部权限
（6）	Location	可读写对象，描述该节点的物理位置
（7）	Services	只读对象，该数值标识实体所提供的服务集合，初始值为 0，该数值为一个合计值

表 2　MIBII interfaces 组 ifNumber 节点描述

节点标识	对 象 名 称	对 象 描 述
（1）	ifNumber	只读，表示一个系统设备的网络接口数（与接口状态无关），OID 为.1.3.6.1.2.1.2.1
（2）	ifTable	接口信息列表，接口的编号值由 ifNumber（总接口数）来提供

表 3　MIBII interfaces 组 ifTable 节点描述

节点标识	对 象 名 称	对 象 描 述
（1）	Index	只读，标识接口的唯一值，取值范围为 1 到总的接口数量。该接口值为常量，在实体网络管理系统重新安装后，该值仍然保持不变
（2）	Descr	只读的显示串，接口的文本描述，描述了接口的厂商名、产品名和硬件接口的版本号（OID 为.1.3.6.1.2.1.2.2.1.2）
（3）	Type	用于描述接口的类型，存储于网络层之下的物理链路层协议栈
（4）	Mtu	Mtu（Memory Transfer Unit，转储单元），只读，接口可以接收或转发的最大数据报（大小按标准八位字节计算）。用于传送网络数据报，该大小值是该接口能传送的最大网络数据报
（5）	Speed	只读，接口当前速率的估算值，为每秒通过的比特数，适用于那些流量较为稳定或者无法精确估算带宽的接口
（6）	PhysAddress	只读，接口物理地址，存储于网络层之下的协议栈

表 5　MIBII IP 组节点描述

节点标识	对 象 名 称	对 象 描 述
（1）	Forwarding	读写，指示出该实体是否担任 IP 网关转发接收到的数据报。该实体作为网关则转发数据报，作为 IP 主机则不转发
（2）	DefaultTTL	TTL（Time To Live，生存时间），可读写，当传输层协议不提供生存时间值时，该值作为默认值插入到该实体发起的数据报 IP 头部分
（3）	InReceives	只读，从接口收到的输入性数据报总数量，包含接收有错误的数据报
（4）	InHdrErrors	只读，由于 IP 报头错误导致被丢弃的输入性数据报总数，包括坏校验，版本号不匹配，其他格式的错误等
（5）	InAddrErrors	只读的计数器，实体接收到数据报中由于 IP 数据报头中目的 IP 地址不是有效地址而丢弃的数据报总数，这个地址包含无效地址（例如 0.0.0.0）和（仅作为实验和开发用的 E 类 IP 地址）
（6）	ForwDatagrams	只读，该实体地址不作为该网络最终目的地址或担任 IP 网关，其他设备将寻找其他途径作为它们的最终目的地，此计数器只记录该实体作为源路由且处理成功的输入性数据报
（7）	InUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol，只读，由于一个未知或不支持的协议而被丢弃的输入数据报数量
（8）	InDiscards	只读，输入的 IP 数据报，虽然没有发生防止其操作的问题，但仍被丢弃的数据报数量（例如，由于缺乏足够缓冲空间而丢弃的数据报）
（9）	InDelivers	只读，输入的 IP 数据报中，成功交付给 IP 用户协议（包括 ICMP 协议）的总数
（10）	OutRequests	只读，本地 IP 用户协议（包括 ICMP 协议），要求传输的 IP 数据报总数
（11）	OutDiscards	只读，输出的 IP 数据报，虽然并没有发生防止其操作的问题，但仍被丢弃的数据报数量（例如，由于缺乏足够缓冲空间而丢弃的数据报）
（12）	OutNoRoutes	只读，因为没有找到路由将其转交给的目的地址而丢弃的数据报
（13）	ReasmTimeout	只读，重组接收到的碎片可等待的最大秒数
（14）	ReasmReqds	只读，接收到的需要重组的 IP 碎片数
（15）	ReasmOKs	只读，成功重组的 IP 数据报数
（16）	ReasmFails	只读，由于 IP 重组算法检测到的重组失败的数据报数
（17）	FragOKs	只读，成功拆分的 IP 数据报数
（18）	FragFails	只读，不能成功拆分而被丢弃的 IP 数据报数
（19）	FragCreates	只读，该实体产生的 IP 数据报报碎片数
（20）	AddrTable	只读，该实体的 IP 地址信息
（21）	RouteTable	实体的 IP 路由表
（22）	NetToMediaTable	将 IP 地址映射到物理地址的地址转换表
（23）	RoutingDiscards	被丢弃的路由选择数量

表 6　MIBII ICMP 组节点描述

节点标识	对 象 名 称	对 象 描 述
（1）	InMsgs	只读，接收到的 ICMP 消息的总数
（2）	InErrors	只读，接收的有错的 ICMP 消息数
（3）	InDestUnreachs	只读，收到的目的 IP 不可达的消息数

续表

节点标识	对 象 名 称	对 象 描 述
（13）	ConnTable	包含 TCP 各个连接的信息
（14）	InErrs	只读，收到的有错的 Segments 总数
（15）	OutRsts	只读，发出的含有 RST 标志的 Segments 总数

表 8　MIBII UDP 组节点描述

节点标识	对 象 名 称	对 象 描 述
（1）	RtoAlgorithm	只读，重传时间
（2）	RtoMin	只读，重传时间的最小值
（3）	RtoMax	只读，重传时间的最大值
（4）	MaxConn	只读，实体支持的 TCP 连接数的上限
（5）	ActiveOpens	只读，实体已经支持的主动打开的数量
（6）	PassiveOpens	只读，实体已经支持的被动打开的数量
（7）	AttemptFails	只读，已经发生的试连失败的次数
（8）	EstabResets	只读，已经发生的复位的次数
（9）	CurrEstab	只读，当前状态为 Established 的 TCP 连接数
（10）	InSegs	只读，收到的 Segments 总数
（11）	OutSegs	只读，发出的 Segmetns 总数
（12）	RetransSegs	只读，重传的 Segmetns 总数
（13）	ConnTable	包含 TCP 各个连接的信息
（14）	InErrs	只读，收到的有错的 Segments 的总数
（15）	OutRsts	只读，发出的含有 RST 标志的 Segments 总数

表 9　MIBII UDP 组节点描述

节点标识	对 象 名 称	对 象 描 述
（1）	InDatagrams	只读，提交该 UDP 用户的数据报总数
（2）	NoPorts	只读，收到的目的端口上没有应用的数据报总数
（3）	InErrors	只读，收到的无法递交的数据包总数
（4）	OutDatagrams	只读，该实体发出的 UDP 数据报总数
（5）	Table	包含 UDP 的用户信息
（6）	localAddress	只读，UDP 用户的本地 IP 地址
（7）	localport	只读，UDP 用户的本地端口号

表 10　MIBII EgpGroup 组节点描述

节点标识	对 象 名 称	对 象 描 述
（1）	InDatagrams	只读，提交该 UDP 用户的数据报总数
（2）	NoPorts	只读，收到的目的端口上没有应用的数据报总数
（3）	InErrors	只读，收到的无法递交的数据包总数
（4）	OutDatagrams	只读，该实体发出的 UDP 数据报总数

续表

节点标识	对 象 名 称	对 象 描 述
（5）	Table	包含 UDP 的用户信息
（6）	localAddress	只读，UDP 用户的本地 IP 地址
（7）	localport	只读，UDP 用户的本地端口号

表 11　MIBII SNMP 组节点描述

节点标识	对 象 名 称	对 象 描 述
（1）	InPkts	传送至 SNMP 实体的消息总数量
（2）	OutPkts	由 SNMP 实体发送出的 SNMP 消息总数量
（3）	InBadVersions	发送至 SNMP 实体的消息中由一个不被网络支持 SNMP 版本所发出的消息总数量
（4）	InBadCommunityNames	发送至 SNMP 实体的消息中使用了错误社区字符串的消息总数量
（5）	InBadCommunityUses	发送至 SNMP 实体的消息就是代表了一种 SNMP 操作请求消息，其中不属于 SNMP 指定范围内操作请求的消息总数量
（6）	InASNParseErrs	SNMP 实体在对接收到的 SNMP 消息进行解码时发生 ASN.1（网络信息格式规范）和 BER（误码率）的总次数
（7）	InTooBigs	发送至 SNMP 实体的消息，消息数据包中“错误状态”位被标识为 Toobigs 的 PDU 总数
（8）	InNoSuchNames	发送至 SNMP 实体的消息，消息数据包中“错误状态”位被标识为 noSuchName 的 PDU 总数
（9）	InBadValues	发送至 SNMP 实体的消息，消息数据包中“错误状态”位被标识为 badValue 的 PDU 总数
（10）	InReadOnlys	发送至 SNMP 实体的消息，消息数据包中“错误状态”位被标识为 readOnly 的 PDU 总数
（11）	InGenErrs	发送至 SNMP 实体的消息，消息数据包中“错误状态”位被标识为 genErr 的 PDU 总数
（12）	InTotalReqVars	SNMP 实体通过 Get-Request 和 Get-Next 命令成功检索的 MIB 数据对象总数量
（13）	InTotalSetVars	SNMP 实体通过 Set-Request 命令成功配置的 MIB 数据对象总数量
（14）	InGetRequests	SNMP 实体接收并处理的 Get-Request 请求类 PUD 总数量
（15）	InGetNexts	SNMP 实体接收并处理的 Get-Next 请求类 PUD 总数量
（16）	InSetRequests	SNMP 实体接收并处理的 Set-Request 类 PUD 总数量
（17）	InGetResponses	SNMP 实体接收并处理的 Get-Response 类 PUD 总数量
（18）	InTraps	SNMP 实体接收并处理的 Trap 类 PUD 总数量
（19）	OutTooBigs	由 SNMP 实体发出的 PDU 数据包中，“错误状态”位标识为 tooBig 的 PDU 总数据
（20）	OutNoSuchNames	由 SNMP 实体发出的 PDU 数据包中，“错误状态”位标识为 noSuchName 的 PDU 总数量
（21）	OutBadValues	由 SNMP 实体发出的 PDU 数据包中，“错误状态”位标识为 badValue 的 PDU 总数量
（22）	OutGenErrs	由 SNMP 实体发出的 PDU 数据包中，“错误状态”位标识为 genErr 的 PDU 总数量

续表

节点标识	对 象 名 称	对 象 描 述
（23）	OutGetRequests	由 SNMP 实体发出的 Get-Request 类 PDU 数据包总数量
（24）	OutGetNexts	由 SNMP 实体发出的 Get-Next 类 PDU 数据包总数量
（25）	OutSetRequests	由 SNMP 实体发出的 Set-Request 类 PDU 数据包总数量
（26）	OutGetResponses	由 SNMP 实体发出的 Get-Response 类 PDU 数据包总数量
（27）	OutTraps	由 SNMP 实体发出的 Trap 类 PDU 数据包总数量
（28）	EnableAuthenTraps	指明允许或者禁止 SNMP 代理是发出身份验证错误的 Trap 信息